Installation et configuration d'ADOBE® CONNECT™ 7.5 SERVICE PACK 1



Adobe Systems Incorporated, 345 Park Avenue, San Jose, California 95110, USA.

Sommaire

Chapitre 1 : Préparation de la migration, de l'installation et de la configuration

Les techniques que vous utilisez pour installer Adobe® Connect™ 7.5 Service Pack 1 dépendent du type de l'installation que vous effectuez.

Remarque : *Dans certains documents et pages web, ce produit sera référencé par le nouveau nom mentionné ci-dessus, Adobe Connect. Au moment de la rédaction de ce manuel, le produit était encore appelé Adobe Acrobat Connect Pro Server ou Connect Pro. C'est le nom utilisé dans ce manuel.*

- Si vous installez Connect Pro pour la première fois, prenez connaissance des exigences relatives à l'installation, des configurations prises en charge et de la présentation technique figurant dans le présent chapitre. Voir ensuite « Installation de Connect Pro 7.5 SP1 » à la page 27.
- Si vous effectuez une migration vers cette version à partir d'une version Connect Pro antérieure à la version 7.5, suivez les instructions de préparation à la migration avant d'effectuer l'installation (voir « Préparation de la migration » à la page 5). Vous devrez installer Connect Pro 7.5 avant d'installer Connect Pro 7.5 SP1 ; voir « Installation de Connect Pro 7.5 (utilisateurs effectuant une migration uniquement) » à la page 22.
- Si vous effectuez une mise à niveau de Connect Pro 7.5 vers Connect Pro 7.5 SP1, consultez les informations ci-dessous qui présentent les nouveautés de cette version. Voir ensuite « Installation de Connect Pro 7.5 SP1 » à la page 27.

Nouveautés de Connect Pro 7.5 SP1

Les fonctionnalités suivantes sont nouvelles ou ont été modifiées dans Connect Pro 7.5 SP1 :

Installation simplifiée des adaptateurs de téléphonie Le programme d'installation permet maintenant d'installer un ou plusieurs adaptateurs de téléphonie. Dans les versions antérieures, vous deviez modifier manuellement certains fichiers XML pour activer et configurer les adaptateurs. La nouvelle version du programme d'installation met à jour ces fichiers, si bien que vous n'avez plus à les modifier manuellement. Par ailleurs, vous n'avez plus à télécharger les fichiers ou les utilitaires des adaptateurs car ils sont inclus dans le programme d'installation. Pour connaître les informations que vous devez avoir à disposition avant l'installation d'un adaptateur, voir « Préparation de l'installation des adaptateurs de téléphonie intégrés » à la page 17.

Le programme d'installation implémente les paramètres d'adaptateur de téléphonie de base. Pour personnaliser un adaptateur après son installation, voir la TechNote à l'adresse www.adobe.com/go/learn_cnn_customize_adaptor_fr.

Fonctionnalités supplémentaires d'adaptateur de téléphonie Les fonctionnalités suivantes sont maintenant prises en charge dans les adaptateurs spécifiés. Pour obtenir des informations relatives à l'implémentation de ces fonctionnalités, voir la TechNote à l'adresse www.adobe.com/go/learn_cnn_customize_adaptor_fr.

- Fusion des jetons : PGi NA, PGi EMEA, InterCall
- Atelier audio Web : Avaya, PGi NA, PGi EMEA, InterCall
- E164 : InterCall et MeetingOne
- Mise en silence de la conférence : MeetingOne

Ajouts aux fonctionnalités de services web Connect Pro permet d'accéder à des services web que les clients peuvent appeler pour échanger des données avec des comptes Connect Pro. Différentes API de téléphonie permettant de gérer des profils et des fournisseurs sont maintenant disponibles. Pour plus d'informations, voir la section concernant l'Utilisation des services web d'Adobe Connect Pro 7.5 Service Pack 1.

Documentation améliorée pour l'implémentation d'adaptateurs de téléphonie personnalisés Pour obtenir des instructions sur l'élaboration de votre propre adaptateur de téléphonie, notamment sur l'outil Javadoc associé, voir Building Telephony Integration with Adobe Connect 7.5 Service Pack 1.

Nouveautés de Connect Pro 7.5

Les fonctionnalités suivantes sont nouvelles ou ont été modifiées dans Connect Pro 7.5 :

VMWare Connect Pro 7.5 ajoute une assistance technique pour l'installation dans un environnement VMWare. Pour plus d'informations, voir le livre blanc relatif à la configuration VMWare et la configuration système Connect Pro.

Universal Voice La solution Universal Voice de Connect Pro 7.5 vous permet de diffuser par VoIP une conférence audio en direct pour des participants à une réunion. Vous pouvez également enregistrer la conférence audio en direct avec la réunion Connect Pro.

Pour déployer la solution Universal Voice, installez et configurez Adobe Flash Media Gateway avec votre installation Connect Pro 7.5. Flash Media Gateway est intégré dans le programme d'installation de Connect Pro 7.5. Flash Media Gateway permet d'établir la communication entre Connect Pro 7.5 et votre infrastructure SIP. Vous pouvez installer Flash Media Gateway sur le même serveur que Connect Pro 7.5 ou sur un autre ordinateur. Reportez-vous à la section « Déploiement de la fonctionnalité de voix universelle » à la page 49.

***Remarque :** outre Universal Voice, Connect Pro 7.5 prend également en charge les adaptateurs de téléphonie entièrement intégrés avec contrôle d'appel avancé et commentaires des participants. Pour plus d'informations, consultez la section « Options de conférence audio Connect Pro » à la page 16.*

Partage des fichiers PDF Adobe® Partagez des fichiers PDF dans des salles de réunion. Dans une salle de réunion, sélectionnez dans la bibliothèque de contenu Connect Pro Central ou dans votre ordinateur les fichiers PDF que vous souhaitez partager. Dans la bibliothèque de contenu, les fichiers PDF sont stockés sous forme de fichiers PDF. Pour être affichés dans la salle de réunion, les fichiers PDF sont convertis en fichiers SWF. Pour plus d'informations, reportez-vous à Partage d'un document.

Assistance améliorée Microsoft® PowerPoint Partagez dans des salles de réunion haute fidélité des documents PPTX qui contiennent des graphiques SmartArt, des tableaux, du texte et des effets de forme. Les présentateurs peuvent télécharger des documents PPTX dans des salles de réunion haute fidélité depuis des systèmes d'exploitation Windows ou Mac.

Connect Pro Add-in pour IBM Lotus Notes Planifiez et gérez les réunions Connect Pro depuis Lotus Notes. Pour plus d'informations, reportez-vous au manuel d'installation et de déploiement d'Adobe Acrobat Connect Pro Add-in pour IBM Lotus Notes et à la section Utilisation d'Adobe Acrobat Connect Pro Add-in pour IBM Lotus Notes.

Liens Prise en charge et Etat du menu d'aide de la salle de réunion Utilisez les paramètres de configuration du fichier custom.ini pour ajouter les options Prise en charge et Etat au menu d'aide de la salle de réunion. Indiquez les URL qui permettent aux utilisateurs de la réunion de consulter les informations relatives aux options de prise en charge et d'état du système. Vous pouvez utiliser les services Web de Connect Pro pour créer une page contenant des informations dynamiques sur l'état du système. Pour plus d'informations, reportez-vous à la section « Ajout de liens Prise en charge et Etat au menu d'aide » à la page 62.

Configuration requise pour l'installation

Configuration matérielle, logicielle et utilisateur

Pour connaître la configuration requise pour Connect Pro et Connect Pro Edge Server , visitez le site www.adobe.com/go/connect_sysreqs_fr.

Configuration des ports

Le tableau suivant décrit les ports sur lesquels les utilisateurs doivent pouvoir établir des connexions TCP.

Chiffre	Adresse de liaison	Accès	Protocole
80	*/Adaptateur quelconque	Public	HTTP, RTMP
443	*/Adaptateur quelconque	Public	HTTPS, RTMPS
1935	*/Adaptateur quelconque	Public	RTMP

Remarque : *RTMP (Real-Time Messaging Protocol) est un protocole Adobe.*

Le tableau suivant décrit les ports ouverts à l'intérieur d'un cluster. Chaque serveur Connect Pro d'un cluster doit pouvoir établir des connexions TCP vers tous les autres serveurs du cluster sur ces ports.

Remarque : *ces ports ne doivent pas être ouverts au public, même si vous n'utilisez pas de cluster.*

Chiffre	Port source	Adresse de liaison	Accès	Protocole
8506	Valeur quelconque	*/Adaptateur quelconque	Privé	RTMP
8507	Valeur quelconque	*/Adaptateur quelconque	Privé	HTTP

Chaque serveur Connect Pro d'un cluster doit pouvoir établir une connexion TCP vers le serveur de base de données sur le port suivant :

Chiffre	Port source	Accès	Protocole
1433	Valeur quelconque	Privé	TSQL

Le tableau suivant décrit les ports serveur utilisés par Connect Pro pour communiquer en interne. Ces ports ne doivent pas être utilisés par un autre processus ou programme sur un serveur hébergeant Connect Pro ; sinon, ce dernier risque de ne pas démarrer.

Chiffre	Adresse de liaison	Accès	Protocole
1111	127.0.0.1	Interne	RTMP
2909	127.0.0.1	Interne	RMI
4111	*/Adaptateur quelconque	Interne	JMX
8510	127.0.0.1	Interne	HTTP

Si vous installez un adaptateur de téléphonie intégré ou personnalisé, le port suivant de chaque Connect Pro Server doit être disponible :

Chiffre	Adresse de liaison	Accès	Protocole
9080	*/Adaptateur quelconque	Public si vous utilisez l'adaptateur de téléphonie InterCall ; interne dans les autres cas	HTTP

Certains adaptateurs de téléphonie intégrés doivent accéder à des ports spécifiques, outre les ports répertoriés dans les tableaux ci-dessus. Ces ports sont répertoriés dans les informations de chaque adaptateur ; voir « Préparation de l'installation des adaptateurs de téléphonie intégrés » à la page 17.

Pour plus d'informations sur les ports Flash Media Gateway, reportez-vous à la section « Ports et protocoles Flash Media Gateway » à la page 50.

Configurations prises en charge

Configurations de bases de données/serveur prises en charge

Connect Pro stocke les informations sur les utilisateurs et le contenu dans une base de données. Configurations de Connect Pro et de bases de données prises en charge :

Serveur unique avec moteur de base de données intégré Installez Connect Pro sur un ordinateur et installez le moteur de base de données intégré (inclus dans le programme d'installation de Connect Pro) sur ce même ordinateur. Le moteur de base de données intégré est Microsoft® SQL Server 2005 Express Edition.

Remarque : *cette configuration ne peut être utilisée que dans des environnements de test, pas dans des environnements de production.*

Serveur unique avec la base de données SQL Server 2005 Standard Edition Installez Connect Pro sur un seul ordinateur et installez Microsoft SQL Server 2005 Standard Edition sur le même ordinateur.

Serveur unique avec la base de données externe SQL Server 2005 Standard Edition Installez Connect Pro sur un seul ordinateur et installez SQL Server 2005 Standard Edition sur un autre ordinateur.

Serveur unique avec les bases de données externes multiples SQL Server 2005 Standard Edition Installez Connect Pro sur un seul ordinateur et installez SQL Server 2005 Standard Edition sur plusieurs ordinateurs (autrement dit un cluster) externes à Connect Pro. Connect Pro prend en charge la copie miroir et la mise en clusters des bases de données SQL Server.

Serveurs multiples avec la base de données externe SQL Server 2005 Standard Edition Installez Connect Pro sur plusieurs ordinateurs (autrement dit un cluster) et installez SQL Server 2005 Standard Edition sur un autre ordinateur.

Serveurs multiples avec les bases de données externes multiples SQL Server 2005 Standard Edition Installez Connect Pro sur plusieurs ordinateurs (autrement dit un cluster) et installez SQL Server 2005 Standard Edition dans un cluster distinct. Connect Pro prend en charge la copie miroir et la mise en clusters des bases de données SQL Server.

Remarque : *Microsoft SQL 2005 Standard Edition n'est pas fourni avec Connect Pro Server et doit être acheté séparément.*

Déploiements de Flash Media Gateway pris en charge

Déployez Flash Media Gateway pour activer Universal Voice. La liste suivante répertorie les déploiements pris en charge :

Un seul ordinateur Installez Connect Pro, Flash Media Gateway et SQL Server sur le même ordinateur.

Deux ordinateurs Installez Connect Pro et Flash Media Gateway sur le même ordinateur et SQL Server sur un autre ordinateur.

Cluster d'ordinateurs Installez chaque instance de Connect Pro et de Flash Media Gateway sur son propre ordinateur.

Voir aussi

« Options de conférence audio Connect Pro » à la page 16

« Déploiement de la fonctionnalité de voix universelle » à la page 49

Serveurs d'annuaire LDAP pris en charge

Vous pouvez configurer l'authentification utilisateur sur le serveur d'annuaire LDAP de votre société et en importer les informations d'annuaire dans Connect Pro. Vous trouverez la liste des serveurs d'annuaire LDAP pris en charge à l'adresse www.adobe.com/go/connect_sysreqs_fr.

Remarque : *tout serveur de répertoire LDAP v.3 peut s'intégrer avec Connect Pro . Toutefois, seuls les serveurs de répertoire qui ont été testés par Adobe sont pris en charge.*

Voir aussi

« Intégration dans un service d'annuaire » à la page 41

Périphériques de stockage de contenu pris en charge

Vous pouvez configurer votre système Connect Pro pour qu'il stocke le contenu sur des périphériques NAS (Network Attached Storage) et SAN (Storage Area Network). Vous trouverez la liste des périphériques NAS et SAN pris en charge à l'adresse www.adobe.com/go/connect_sysreqs_fr.

Voir aussi

« Configuration du stockage partagé » à la page 59

Préparation de la migration

Voies de migration

Exécutez le programme d’installation de Connect Pro 7.5 pour effectuer la mise à niveau de Connect Pro 7.x vers Connect Pro 7.5. Exécutez ensuite le programme d’installation de Connect Pro 7.5 SP1. Cette procédure est le seul chemin de mise à niveau. Le programme d’installation de Connect Pro et la Console de gestion des applications fournissent des interfaces utilisateur graphiques qui vous guident dans la mise à niveau.

Pour plus d'informations sur la mise à niveau, contactez l'assistance d'Adobe : www.adobe.com/go/connect_licensed_programs_fr.

Migration de Connect Pro 7.x vers Connect Pro 7.5 SP1

Suivez ce processus pour effectuer la migration de Connect Pro 7.x vers Connect Pro 7.5 SP1.

Remarque : *Comme l’indiquent les étapes ci-dessous, vous installez Connect Pro 7.5 avant d’installer Connect Pro 7.5 SP1.*

1. Testez la migration dans un environnement non destiné à la production.

Il est généralement conseillé de prendre un instantané de l'environnement de production actuel et de tester la migration dans un environnement de test avant de migrer l'environnement de production. Lorsque vous avez réussi la migration dans l'environnement test, passez à l'étape 2.

2. Informez les utilisateurs quant à la migration.

Reportez-vous à la section « Information des utilisateurs quant à la migration » à la page 6.

3. (Facultatif) Sauvegardez le contenu et les fichiers de configuration.

Reportez-vous à la section « Sauvegarde des fichiers » à la page 6.

4. Sauvegardez la base de données.

Reportez-vous à la section « Sauvegarde de la base de données » à la page 117.

5. Exécutez le programme d'installation de Connect Pro 7.5.

Voir « Installation de Connect Pro 7.5 (utilisateurs effectuant une migration uniquement) » à la page 22. Le programme d'installation arrête les services Connect Pro et sauvegarde les fichiers existants, y compris le fichier custom.ini.

(Facultatif) Réunissez les informations nécessaires pour installer un ou plusieurs adaptateurs de téléphonie intégrés.

Voir « Préparation de l'installation des adaptateurs de téléphonie intégrés » à la page 17.

Exécutez le programme d'installation Connect Pro 7.5 SP1.

Voir « Installation de Connect Pro 7.5 SP1 » à la page 27.

1. Vérifiez votre installation.

Reportez-vous à la section « Vérification de l'installation » à la page 30.

Information des utilisateurs quant à la migration

Comme pour toute mise à niveau logicielle, et en particulier si elle affecte un groupe de travail, la communication et la planification sont importantes. Avant de démarrer la migration ou l'ajout de modules à Connect Pro, Adobe vous suggère d'effectuer les opérations suivantes :

- Prévoyez suffisamment de temps pour assurer une migration réussie. Il est préférable d'effectuer la mise à niveau pendant la période de maintenance habituelle.
- Signalez à vos utilisateurs qu'ils ne pourront pas utiliser Connect Pro pendant la migration.
- Informez-les également des types de changements auxquels ils doivent s'attendre (nouvelles fonctionnalités ou meilleures performances, par exemple) après la migration. Pour plus d'informations sur les nouvelles fonctionnalités, visitez le site www.adobe.com/go/learn_cnn_whatsnew_fr.

Sauvegarde des fichiers

Le programme d'installation crée des copies de sauvegarde des répertoires appserv et comserv, ainsi que du fichier custom.ini, et installe les nouvelles versions. Le répertoire de contenu n'est ni effacé ni écrasé par le programme d'installation.

Vous pouvez choisir de créer des copies de sauvegarde de ces répertoires et fichiers.

Mise à niveau depuis SQL Server 2005 Express Edition

Procédez comme suit pour migrer de l'utilisation de la base de données intégrée à celle de SQL Server 2005 Standard Edition sur un autre ordinateur.

Remarque : *Vous pouvez effectuer cette migration lorsque vous migrez d'Adobe Connect 7.x vers Connect Pro 7.5 SP1. Vous pouvez également le faire à tout moment après avoir installé Connect Pro 7.5 SP1.*

1. Installez SQL Server 2005 Standard Edition sur un ordinateur différent de celui hébergeant Connect Pro.

Suivez les instructions fournies par Microsoft pour installer SQL Server.

2. Sauvegardez SQL Server 2005 Express Edition.

Reportez-vous à la section « Sauvegarde de la base de données » à la page 117.

3. Copiez le fichier BAK depuis l'ordinateur hébergeant Connect Pro sur l'ordinateur qui héberge SQL Server.

Lorsque vous sauvegardez SQL Server Express Edition, un fichier nommé *breeze*.bak est créé (où *breeze* correspond au nom de la base de données).

4. Rétablissez la base de données sur l'ordinateur qui héberge SQL Server 2005 Standard Edition.

Pour plus d'informations sur le rétablissement de SQL Server, consultez Microsoft TechNet.

5. Entrez les informations relatives à la base de données SQL Server 2005 Standard Edition dans la Console de gestion des applications sur le serveur qui héberge Connect Pro.

Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server > Configurer Connect Pro Server.

Préparation de l'installation de Connect Pro

Présentation technique de Connect Pro

Une installation de Connect Pro se compose de plusieurs éléments : Connect Pro Central Application Server, Adobe® Flash® Media Server, Connect Pro Presence Service, Flash Media Gateway (Universal Voice), une base de données et des adaptateurs de téléphonie pour la conférence audio.

Connect Pro Central Application Server est fondé sur la spécification J2EE et utilise des composants de Macromedia® JRun™ d'Adobe. Egalement appelé *serveur d'application*, il gère les utilisateurs, les groupes, le contenu à la demande et les sessions des clients. Parmi les tâches du serveur d'applications, on retrouve le contrôle d'accès, la sécurité, les quotas, les licences et les fonctions d'audit et de gestion, telles que la mise en cluster, le basculement et la réplication. Il transcode également les supports, en convertissant notamment les éléments Microsoft® PowerPoint et le son au format Adobe® Flash®. Le serveur d'applications gère les requêtes de réunion et de transfert de contenu (diapositives, pages HTTP, fichiers SWF et contenu du module Partage de fichiers) sur une connexion HTTP ou HTTPS.

Certains composants de Flash Media Server, également appelé *serveur de réunions*, sont installés avec Connect Pro pour la gestion de la diffusion audio et vidéo en temps réel, la synchronisation des données et la diffusion des contenus multimédia, ainsi que les interactions avec les réunions Connect Pro. Certaines tâches de Flash Media Server consistent à enregistrer et lire des réunions, à synchroniser le contenu audio et vidéo et à faire le transcodage (conversion et compression des données pour le partage d'écran en temps réel et les interactions). Flash Media Server réduit également la charge et les délais d'attente du serveur en mettant en cache les pages Web fréquemment visitées, les flux continus et les données partagées. Flash Media Server diffuse le son, la vidéo et les données de réunions associées via le protocole à haute performance RTMP ou RTMPS d'Adobe.

Connect Pro Presence Service intègre Connect Pro avec Microsoft® Live Communications Server 2005 et Microsoft® Office Communications Server 2007 pour afficher leur présence en messagerie instantanée dans les salles de réunion Connect Pro. Vous pouvez choisir d'installer Presence Service pendant l'installation.

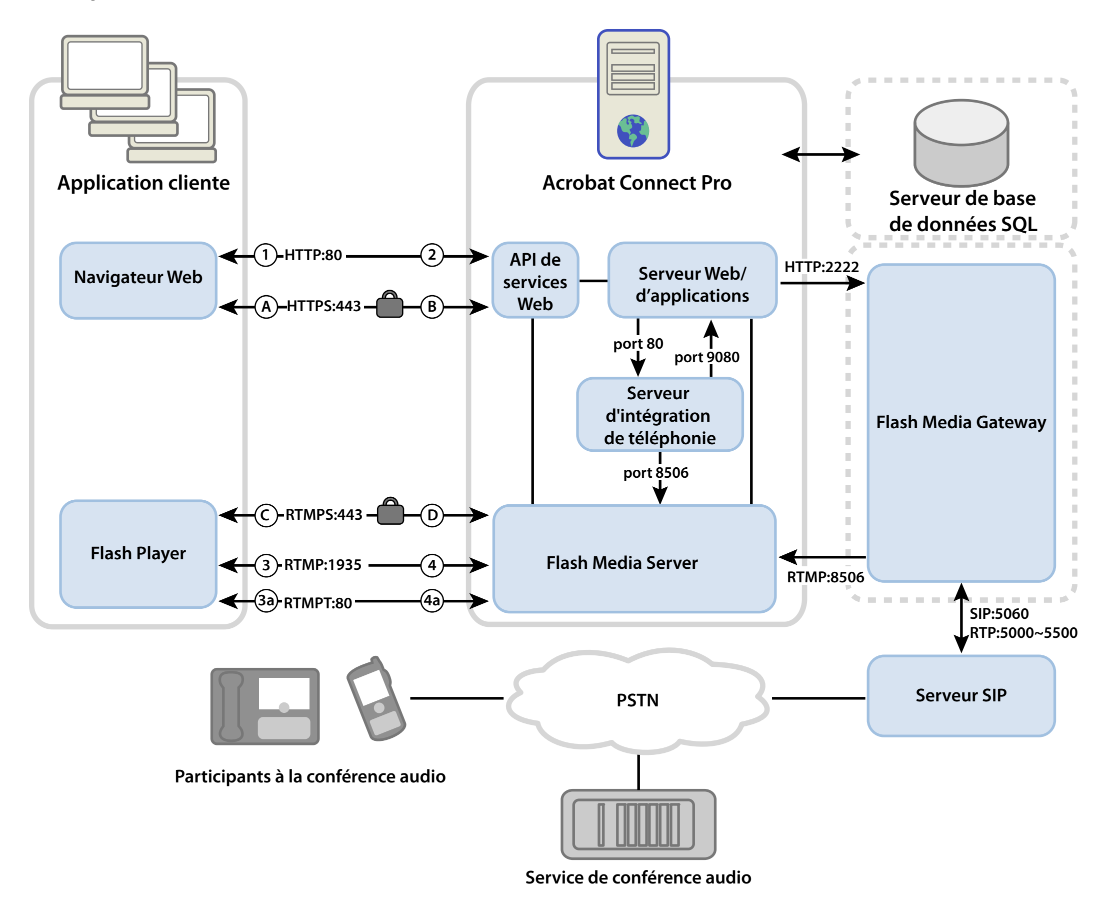
Flash Media Gateway intègre Connect Pro avec votre infrastructure SIP/RTP. Flash Media Gateway reçoit le son d'un serveur SIP et l'envoie aux salles de réunion Connect Pro. Cette solution s'appelle la voix universelle.

Connect Pro requiert une base de données pour le stockage permanent des métadonnées transactionnelles et d'application, dont les informations sur les utilisateurs, les groupes, le contenu et les rapports. Vous pouvez utiliser le moteur de la base de données intégrée (SQL 2005 Express Edition) inclus dans le programme d'installation Connect Pro Server ou vous pouvez acheter et installer Microsoft SQL Server 2005 Standard Edition.

Connect Pro prend en charge plusieurs adaptateurs de téléphonie pour activer les conférences audio. Vous pouvez choisir d'installer un ou plusieurs adaptateurs pendant l'installation.

Flux de données

Le diagramme suivant illustre la circulation des données entre une application cliente et Connect Pro.



Les données peuvent circuler sur une connexion chiffrée ou non chiffrée.

Connexion non chiffrée

Les connexions non chiffrées passent par HTTP et RTMP et empruntent les chemins décrits dans le tableau. Dans le tableau, les numéros correspondent à ceux du diagramme de flux des données.

Chiffre	Description
1	Le navigateur Web du client demande une réunion ou l'URL d'un contenu sur HTTP:80.
2	Le serveur Web répond et transfert le contenu ou fournit au client les informations nécessaires pour qu'il se connecte à la réunion.
3	Le Flash Player du client demande une connexion à la réunion sur RTMP:1935.
3a	Le Flash Player du client demande une connexion à la réunion, mais ne peut se connecter que sur RTMP:80.
4	Flash Media Server répond et ouvre une connexion permanente pour le trafic des flux continus de Connect Pro.
4a	Flash Media Server répond et ouvre une connexion par tunnel pour le trafic des flux continus de Connect Pro.

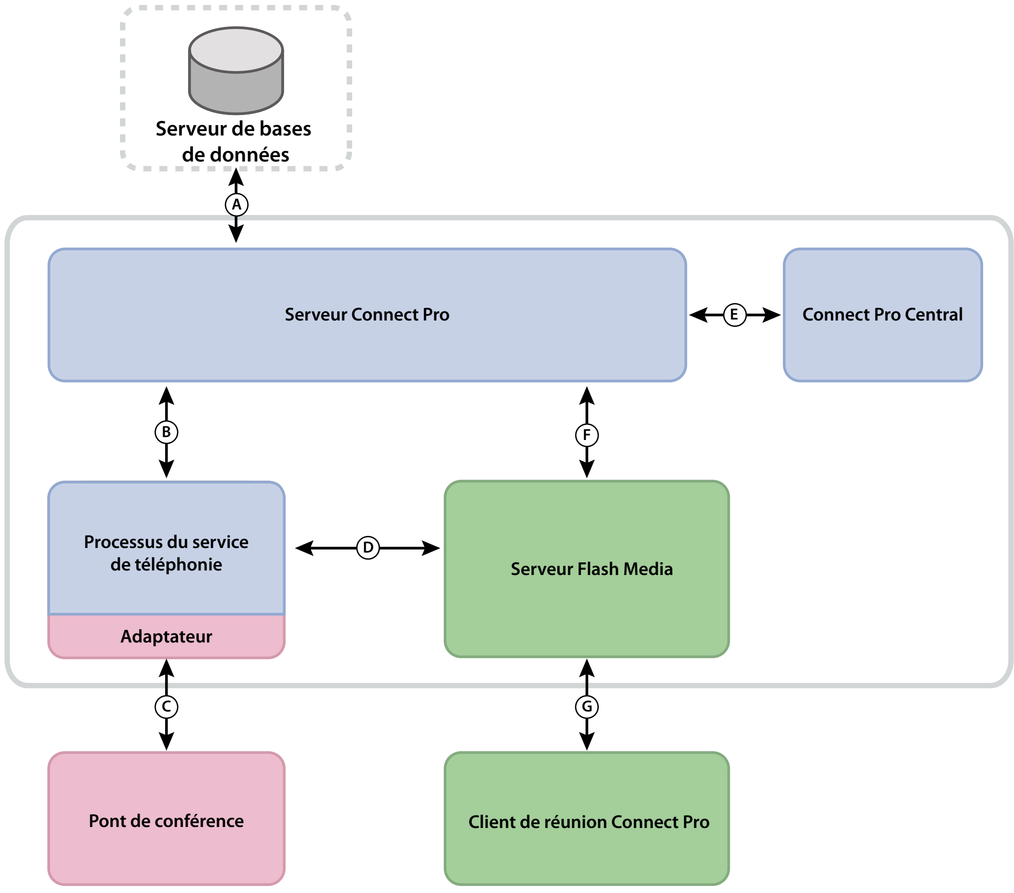
Connexion chiffrée

Les connexions chiffrées passent par HTTPS et RTMPS et empruntent les chemins décrits dans le tableau. Dans le tableau, les lettres correspondent à celles du diagramme de flux des données.

Lettre	Description
A	Le navigateur Web du client requiert une réunion ou l'URL d'un contenu via une connexion sécurisée sur HTTPS:443.
B	Le serveur Web répond et transfert le contenu sur une connexion sécurisée ou fournit au client les informations nécessaires pour qu'il se connecte à la réunion de manière sécurisée.
C	Le Flash Player du client demande une connexion sécurisée à Flash Media Server sur RTMPS:443.
D	Flash Media Server répond et ouvre une connexion permanente et sécurisée pour le trafic des flux continus de Connect Pro.

Flux de données de téléphonie

Le diagramme suivant illustre la circulation des données entre les services de téléphonie et Connect Pro.



A. Connexion permanente. B. Gestion des services et défaillance, connexion de service et courtage de sessions, fourniture des données utilisateur et accès à ces données. C. Commandes natives et événements utilisant les API fournisseur propriétaires pour le contrôle de conférence. D. Commandes et événements utilisant les appels RPC. E. Fourniture. F. Demande de service de téléphonie. G. Commandes de téléphonie et état.

Déroulement de l'installation

La procédure suivante vous aide à concevoir, installer et configurer un système Connect Pro. Certaines étapes vous invitent à prendre des décisions, d'autres requièrent une tâche complète. Chaque étape vous renvoie vers des informations générales sur la décision ou la tâche.

1. Choisissez la base de données que vous souhaitez utiliser.

Pour plus d'informations, consultez la section « Choix d'une base de données » à la page 13.

2. Si vous choisissez d'utiliser SQL Server 2005 Standard Edition à l'étape 1, installez-le.

Pour plus d'informations, consultez la documentation de SQL Server.

Remarque : *Si vous installez la base de données intégrée, vous n'avez pas à suivre cette étape.*

3. (Facultatif) Choisissez et réunissez les informations nécessaires à l'installation des adaptateurs de téléphonie.

Si vous installez un ou plusieurs adaptateurs de téléphonie intégrés, collectez les informations demandées par le programme d'installation. Pour plus d'informations, voir « Choix de l'installation des adaptateurs de téléphonie intégrés » à la page 14.

4. Installez Connect Pro 7.5 sur un seul serveur (utilisateurs effectuant une migration uniquement).

Si vous effectuez une migration à partir de Connect Pro 7.x, installez, configurez et vérifiez Connect Pro 7.5. Pour plus d'informations, voir « Installation de Connect Pro 7.5 (utilisateurs effectuant une migration uniquement) » à la page 22.

5. Installez Connect Pro 7.5 SP1 sur un seul serveur.

Pendant l'installation de Connect Pro 7.5 SP1, vous pouvez également installer le moteur de base de données intégrée, un ou plusieurs adaptateurs de téléphonie, Flash Media Gateway (Universal Voice) et Presence Server. Pour plus d'informations, voir « Installation de Connect Pro 7.5 SP1 » à la page 27.

6. Assurez-vous que Connect Pro est correctement installé.

Pour plus d'informations, consultez la section « Vérification de l'installation » à la page 30.

7. Déployez Connect Pro.

Pour plus d'informations, consultez la section « Déploiement de Connect Pro » à la page 35.

8. (Facultatif) Intégrez Connect Pro à votre infrastructure.

De nombreuses possibilités permettent d'intégrer Connect Pro à l'infrastructure existante de votre société. Il est généralement préférable de vérifier le bon fonctionnement de Connect Pro après la configuration de chacune de ces fonctionnalités.

Intégration avec un fournisseur SIP Intégrez Connect Pro au serveur SIP de votre organisation ou à un fournisseur SIP tiers (également appelé *fournisseur VOIP*) qui fournira une fonctionnalité d'organisation de conférences audio sans interruption. Reportez-vous à la section « Déploiement de la fonctionnalité de voix universelle » à la page 49.

Intégration à un annuaire LDAP Intégrez Connect Pro au serveur d'annuaire LDAP de votre société pour éviter de devoir gérer plusieurs annuaires d'utilisateurs. Reportez-vous à la section « Intégration dans un service d'annuaire » à la page 41.

Configuration d'une couche SSL Sécurisez l'ensemble des communications de Connect Pro. Reportez-vous à la section « Protocole SSL (Secure Sockets Layer) » à la page 81.

Stockage du contenu sur des périphériques NAS/SAN Utilisez des périphériques réseau pour partager les tâches de stockage du contenu. Voir la section « Configuration du stockage partagé » à la page 59.

Intégration à Live Communications Server et Office Communications Server L'intégration à un serveur de communication permet aux hôtes de réunion de voir la présence IM des invités dans les salles de réunion. Les hôtes de réunion peuvent également envoyer des messages aux utilisateurs IM depuis la salle de réunion. Consultez la section « Intégration à Microsoft Live Communications Server 2005 et Microsoft Office Communications Server 2007 » à la page 65.

Configuration d'une infrastructure à clé publique (ICP) Si vous avez intégré Connect Pro à un serveur d'annuaire LDAP, renforcez la sécurité en demandant des certificats clients. Reportez-vous à la section « Infrastructure à clé publique (ICP) » à la page 95.

Hébergement de Connect Pro Add-in Les utilisateurs peuvent très facilement télécharger l'extension Connect Pro Add-in depuis les serveurs d'Adobe. Toutefois, si la stratégie de sécurité de votre société n'autorise pas les téléchargements externes, hébergez l'Add-in sur votre propre serveur pour améliorer le confort de vos utilisateurs. Voir la section « Hébergement d'Acrobat Connect Add-in » à la page 79.

9. (Facultatif) Choisissez d'installer ou non Connect Pro dans un cluster.

Pour plus d'informations, voir « Choix du déploiement de Connect Pro dans un cluster » à la page 12.

10. (Facultatif) Choisissez d'installer ou non des serveurs Edge.

Pour plus d'informations, voir « Choix du déploiement de Connect Pro Edge Server » à la page 14.

Choix du déploiement de Connect Pro dans un cluster

Il est possible d'installer tous les composants Connect Pro , y compris la base de données, sur un seul serveur, mais cette configuration convient mieux à un environnement de test que de production.

Un groupe de serveurs connectés, chacun faisant le même travail, est généralement appelé *cluster*. Dans un cluster Connect Pro , vous installez une copie identique de Connect Pro sur chacun de ses serveurs.

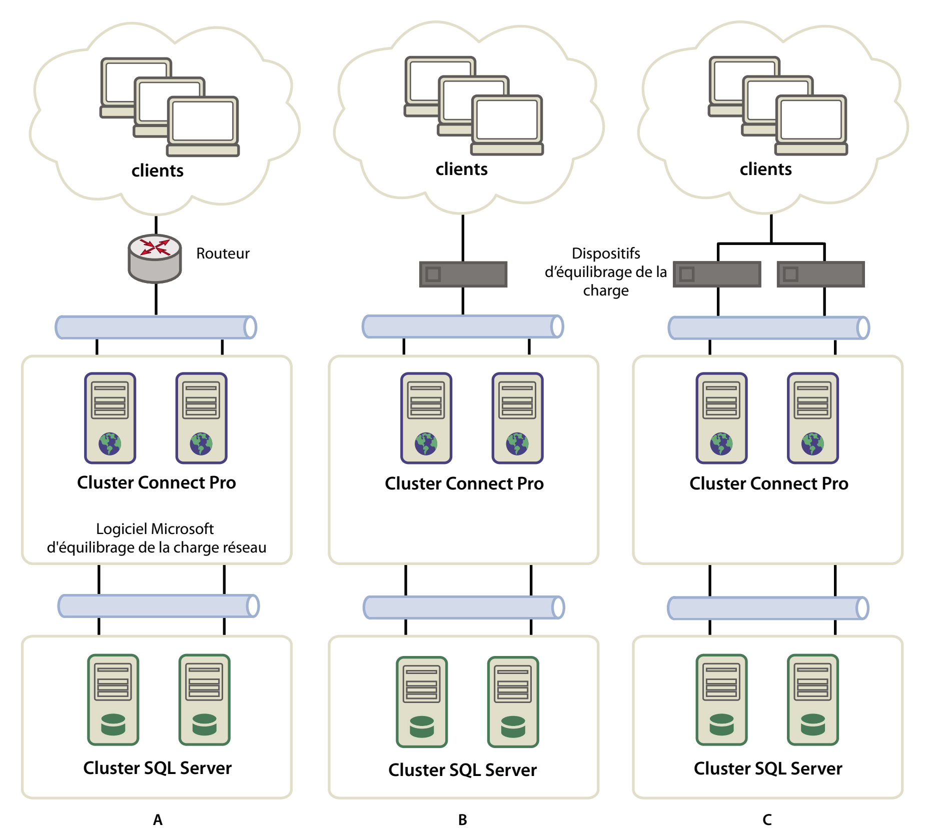
Remarque : *lorsque vous installez Connect Pro dans un cluster, vous devez utiliser SQL Server 2005 Standard Edition et l'installer sur un ordinateur distinct.*

Lorsqu'un hôte du cluster échoue, un autre prend le relais et peut héberger la même réunion. Pour assurer l'équilibrage de charge du cluster, vous devez utiliser un logiciel ou un matériel tiers. Très souvent, le matériel d'équilibrage de charge peut également fonctionner comme un accélérateur SSL.

Remarque : *dans la Console de gestion des applications, vous pouvez configurer un stockage partagé pour que le contenu soit stocké sur des périphériques externes et mis en mémoire cache sur Connect Pro Server.*

Les systèmes réseau fiables sont conçus avec des composants redondants : si l'un échoue, un autre composant identique (*redondant*) prend en charge le même travail. Lorsqu'un composant échoue et qu'un autre prend le relais, un *basculement* intervient.

Idéalement, chaque composant d'un système doit être redondant, pas seulement Connect Pro. Par exemple, vous pourriez utiliser plusieurs périphériques matériels d'équilibrage de charge (BIG-IP de F5 Networks par exemple), un cluster de serveurs hébergeant Connect Pro, ainsi que des bases de données SQL Server sur plusieurs ordinateurs externes. Concevez votre système avec autant de redondances que possible et ajoutez-les progressivement à votre système.



Trois options de mise en cluster
A. *Un cluster avec logiciel d'équilibrage NLB et deux bases de données externes* ***B.*** *Des périphériques d'équilibrage matériel BIG-IP, un cluster et deux bases de données externes* ***C.*** *Deux périphériques d'équilibrage BIG-IP, un cluster et deux bases de données externes*

Voir aussi

« Déployer un cluster de serveurs Connect Pro » à la page 35

« Configuration du stockage partagé » à la page 59

Choix d'une base de données

Connect Pro stocke les informations sur les utilisateurs, le contenu, les cours, les réunions et les rapports dans une base de données. Vous pouvez utiliser le moteur de base de données intégré (inclus avec le programme d'installation) ou installer Microsoft SQL Server 2005 Standard Edition (vendu séparément).

Remarque : *le moteur de base de données intégré est Microsoft SQL Server 2005 Express Edition.*

Base de données intégrée

Le moteur de base de données intégré est recommandé pour les phases de test et de développement. Il utilise les mêmes structures de données que SQL Server 2005 Standard Edition, mais n'est pas aussi puissant.

Le moteur de base de données intégré présente les limites suivantes :

- Du fait des restrictions de licence, vous devez l'installer sur le même ordinateur que Connect Pro. Cet ordinateur doit être mono-processeur.
- La taille maximale de la base de données est de 2 Go.

- Le moteur de base de données intégré possède une interface de ligne de commande, et non une interface utilisateur graphique.

Microsoft SQL Server 2005 Standard Edition

Il est généralement préférable d'utiliser le moteur Microsoft SQL Server 2005 Standard Edition dans les environnements de production, car SQL Server est un système de gestion de bases de données évolutif (SGBDR) conçu pour prendre en charge un grand nombre d'utilisateurs simultanés. SQL Server 2005 Standard Edition fournit également des interfaces utilisateur graphiques pour la gestion et les interrogations de la base de données.

Vous pouvez installer SQL 2005 Standard Edition sur le même ordinateur que Connect Pro Server ou sur un autre ordinateur. Si vous les installez sur des ordinateurs différents, synchronisez ces machines sur la même source horaire. Pour plus d'informations, consultez la TechNote suivante : www.adobe.com/go/2e86ea67.

Installez SQL Server en mode de connexion mixte afin de pouvoir utiliser l'authentification SQL. Définissez la base de données pour respecter la casse.

Utilisez SQL Server dans les scénarios de déploiement suivants :

- Vous souhaitez installer la base de données sur un ordinateur sur lequel Connect Pro n'est pas installé.
- Connect Pro est déployé dans un cluster.
- Connect Pro est installé sur des ordinateurs multi-processeurs avec Hyper-Threading.

Voir aussi

« Configurations de bases de données/serveur prises en charge » à la page 4

Choix de l'installation des adaptateurs de téléphonie intégrés

Pendant l'installation de Connect Pro 7.5 SP1, vous pouvez installer un ou plusieurs adaptateurs de téléphonie.

Pour chaque adaptateur, vous devez fournir des informations spécifiques. Si vous disposez de ces informations, vous pouvez configurer l'adaptateur pendant l'installation initiale de Connect Pro. Si vous préférez, vous pouvez installer l'adaptateur sans le configurer. Lorsque vous êtes prêt à configurer l'adaptateur, exécutez de nouveau le programme d'installation. Pour plus d'informations, voir « Préparation de l'installation des adaptateurs de téléphonie intégrés » à la page 17.

Choix du déploiement de Connect Pro Edge Server

Lorsque vous déployez Connect Pro Edge Server sur votre réseau, les clients se connectent au serveur Edge qui, à son tour, se connecte à Connect Pro (également appelé *serveur d'origine*). Cette connexion est transparente : les utilisateurs ont l'impression de se connecter directement au serveur d'origine qui héberge la réunion.

Les serveurs Edge présentent les avantages suivants :

Latence réseau réduite Les serveurs Edge mettent le contenu en cache à la demande (par exemple les réunions et les présentations enregistrées) et divisent les flux en direct, entraînant moins de trafic vers l'origine. Les serveurs Edge rapprochent les ressources des clients.

Stratégies Les serveurs Edge constituent une couche supplémentaire entre la connexion Internet cliente et l'origine.

Si votre licence l'autorise, vous pouvez installer et configurer un cluster de serveurs Edge. Le déploiement des serveurs Edge dans un cluster présente les avantages suivants :

Basculement Lorsqu'un serveur Edge échoue, les clients sont dirigés vers un autre serveur Edge.

Prise en charge pour des événements importants S'il vous faut plus de 500 connexions simultanées pour la même réunion, un seul serveur Edge n'aura plus assez de sockets. Un cluster autorise davantage de connexions à la même réunion.

Equilibrage de charge S'il vous faut plus de 100 réunions simultanées, un seul serveur Edge peut manquer de mémoire. Les serveurs Edge peuvent être placés en cluster derrière un équilibreur de charge.

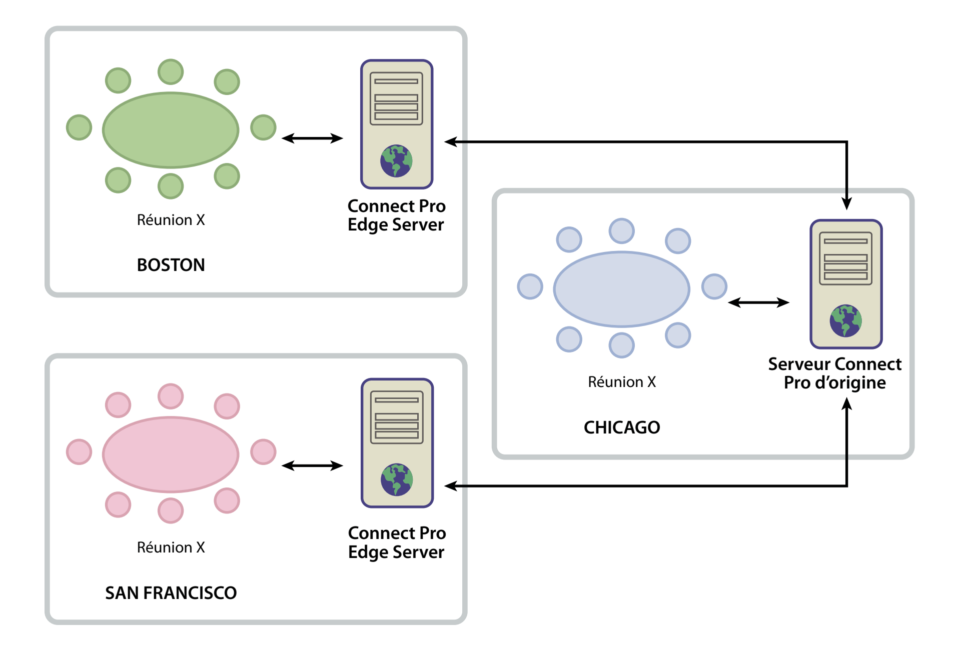
Fonctionnement des serveurs Edge

Les serveurs Edge authentifient les utilisateurs et autorisent leurs requêtes de services Web, telles que Connect Pro Meeting, au lieu de transmettre chaque requête au serveur d'origine et de consommer les ressources de ce dernier pour ces tâches. Si les données demandées sont détectées dans le cache du serveur Edge, ce dernier les envoie au client sans appeler Connect Pro.

Si les données demandées ne sont pas dans le cache du serveur Edge, ce dernier transmet la requête du client au serveur d'origine, où l'utilisateur est authentifié et la demande de services autorisée. Le serveur d'origine renvoie les résultats au serveur Edge, qui les transmet à son tour au client. Le serveur Edge stocke également ces informations dans sa mémoire cache, permettant ainsi à d'autres utilisateurs authentifiés d'y accéder.

Exemple de déploiement de serveur Edge

Considérez l'exemple de déploiement de serveur Edge suivant :



Les clients du site de Chicago utilisent le serveur d'origine situé dans un centre de données de Chicago. Les serveurs Edge de Boston et San Francisco réunissent les requêtes des clients locaux et les transmettent à l'origine. Les serveurs Edge reçoivent les réponses de l'origine à Chicago et les transmettent aux clients de leur régions.

Voir aussi

« Installez Connect Pro Edge Server » à la page 32

« Déploiement de Connect Pro Edge Server » à la page 39

Création et optimisation d'un environnement VMWare

L'installation de Connect Pro sur VMWare ne diffère pas de l'installation sur un ordinateur physique. Pour plus d'informations sur le matériel, les logiciels et la configuration minimum requise, consultez le document technique sur l'exécution de Connect Pro dans un environnement virtuel.

Options de conférence audio Connect Pro

Connect Pro prend en charge deux méthodes de connexion à des fournisseurs de conférences audio : la fonctionnalité Universal Voice et les adaptateurs de téléphonie intégrés. Chaque solution présente des avantages différents. Vous pouvez configurer une solution ou les deux solutions pour un seul fournisseur de conférences audio. Vous pouvez configurer n'importe quel nombre de fournisseurs de conférences audio pour un compte Connect Pro.

La fonctionnalité de **voix universelle** permet à Connect Pro de recevoir du son à partir de n'importe quel fournisseur de conférences audio. Vous pouvez enregistrer le son de votre conférence Web et le transmettre aux participants VoIP uniquement.

La solution de voix universelle utilise un composant appelé Flash Media Gateway qui s'installe avec Connect Pro. Flash Media Gateway reçoit le son d'un serveur SIP et l'envoie à Connect Pro via RTMP. Pour utiliser la fonctionnalité de voix universelle, vous devez héberger votre propre serveur SIP ou disposer d'un compte avec un fournisseur SIP. Pour plus d'informations sur la configuration de Flash Media Gateway, consultez la section « Déploiement de la fonctionnalité de voix universelle » à la page 49.

Après le déploiement de la fonctionnalité Universal Voice, les administrateurs de compte peuvent utiliser Connect Pro Central pour configurer les informations relatives aux conférences audio. Pour plus d’informations, voir www.adobe.com/go/learn_cnn_uvconfig_fr.

Les **adaptateurs de téléphonie intégrés** sont des extensions Java qui fournissent une communication entre Connect Pro et des fournisseurs de conférences audio spécifiques. Les adaptateurs de téléphonie intégrés fournissent un contrôle des appels amélioré. Vous pouvez installer un ou plusieurs adaptateurs de téléphonie lorsque vous installez Connect Pro. Pour plus d'informations, voir « Choix de l’installation des adaptateurs de téléphonie intégrés » à la page 14.

Vous pouvez également utiliser l'API de téléphonie Java Connect Pro Telephony pour développer un adaptateur de téléphonie intégré pour n'importe quel fournisseur de conférences audio. Pour plus d’informations, voir Building Telephony Integration with Adobe Connect 7.5 Service Pack 1.

Le tableau suivant décrit les caractéristiques des deux solutions :

	Fournisseur audio avec fonctionnalité de voix universelle	**Adaptateur de téléphonie intégré**
Diffusion de son aux participants VoIP uniquement	Oui	Non (à moins que l'adaptateur soit configuré pour la fonctionnalité de voix universelle)
Contrôle d'appel amélioré. Par exemple, mise en silence, mise en attente, etc.	Non	Oui
Enregistrement du son avec une réunion Connect Pro	Oui	Oui
Nécessite Flash Media Gateway (intégré dans le programme d'installation de Connect Pro)	Oui	Non (à moins que l'adaptateur soit configuré pour la fonctionnalité de voix universelle)

Préparation de l'installation des adaptateurs de téléphonie intégrés

Les adaptateurs de téléphonie intégrés fournissent la communication entre Connect Pro et des fournisseurs de conférences audio spécifiques. Les adaptateurs intégrés proposent des fonctionnalités d'appel avancées qui permettent aux hôtes et aux présentateurs de contrôler la conférence audio depuis la réunion. Pour chaque adaptateur, vous devez fournir des informations spécifiques pendant l'installation. Pour plus d'informations, voir:

- « Adaptateur de téléphonie Avaya » à la page 17
- « Adaptateur de téléphonie InterCall » à la page 18
- « Adaptateur de téléphonie MeetingOne » à la page 19
- « Adaptateur de téléphonie PGi (auparavant Premiere Global) NA ou EMEA » à la page 20

Remarque : *Vous pouvez activer plusieurs ponts audio pour Connect Pro Server. Les hôtes de réunion sélectionnent le pont audio à utiliser lorsqu'ils créent une réunion dans Connect Pro Central. Chaque réunion ne peut avoir qu'un seul pont audio.*

Adaptateur de téléphonie Avaya

L'adaptateur de téléphonie Avaya Meeting Exchange™ permet aux hôtes et présentateurs des réunions, ainsi qu'aux participants, de contrôler les fonctionnalités de conférence audio depuis les salles de réunion Connect Pro. Réalisez la procédure suivante pour activer l'adaptateur de téléphonie.

Utilisation du service clientèle d'Avaya

Il est recommandé d'intégrer le service clientèle Avaya dans les premières phases de la planification. Assurez-vous que vous disposez des coordonnées du représentant du compte Avaya et du service clientèle Avaya. Contactez l'assistance Avaya pour l'informer que vous installez et utilisez l'adaptateur et pour collecter les informations concernant le pont.

Remarque : *il est nécessaire d'avoir un contrat de maintenance en cours avec Avaya pour le pont audio.*

1 Contactez le service clientèle d'Avaya.

2 Demandez les informations suivantes :

- L'adresse IP du pont

  La communication entre Connect Pro et l'adaptateur de téléphonie s'effectue par l'intermédiaire du pont Avaya.

- Un nom de connexion d'administration

  Utilisez le nom de connexion d'administration pour configurer et redémarrer le pont, modifier le nombre des opérateurs, ajouter de nouveaux utilisateurs et consulter les statistiques.

  Remarque : *Avaya utilise un autre nom de connexion pour l'accès à la racine. Avaya ne fournit généralement pas ce nom de connexion aux clients. Pour les opérations nécessitant un accès à la racine, contactez le service clientèle d'Avaya.*

- Un nom de connexion d'accès aux fichiers

  Utilisez le nom de connexion d'accès aux fichiers pour établir la connexion au répertoire des fichiers d'enregistrement.

- Un nom d'utilisateur et un mot de passe Bridge Talk

Bridge Talk est une application qui gère les conférences et les appelants sur le pont de conférence audio Avaya Meeting Exchange. Utilisez Bridge Talk pour déterminer si le pont ou l'adaptateur présente une défaillance. Vous pouvez également utiliser ce programme pour composer des numéros de téléphone, créer, planifier et gérer de nouvelles conférences, afficher les conférences en cours et surveiller l'activité du pont. Pour plus d'informations, et accéder notamment au guide de l'utilisateur, voir www.avaya.com/fr.

3 Vérifiez que vous disposez d'un accès FTP au répertoire des fichiers d'enregistrement en saisissant les informations suivantes à l'invite FTP :

```
ftp://bridgeIPAddress
ftp>dcbguest:abc123@machineNameOrIPAddress
ftp>cd /usr3/confrp
ftp>bye
```

Informations nécessaires à l'installation

Les éléments repérés par un astérisque (*) sont obligatoires.

Activer l'accès en cours de conférence Sélectionner cette option pour activer l'accès en cours de conférence dans l'intégralité du système. Si vous ne sélectionnez pas cette option, les sélections que vous effectuez pour les quatre entrées suivantes sont ignorées. Si vous sélectionnez cette option, utilisez les quatre options suivantes pour indiquer le mode d'implémentation de l'accès en cours de conférence.

Activer l'accès en cours de conférence pour l'hôte Sélectionner cette option pour autoriser l'accès en cours de conférence à l'hôte de la réunion.

Activer l'accès en cours de conférence pour le présentateur Sélectionner cette option pour autoriser l'accès en cours de conférence au présentateur.

Activer l'accès en cours de conférence pour le participant Sélectionner cette option pour autoriser l'accès en cours de conférence aux participants.

Activer la boîte de dialogue M'appeler Si l'accès en cours de conférence est activé, sélectionnez cette option afin d'afficher la boîte de dialogue M'appeler pour les participants lorsqu'ils rejoignent une réunion.

Nom d'hôte Meeting Exchange* Nom d'hôte ou adresse du serveur Avaya Meeting Exchange.

ID de l'opérateur de téléphonie* ID du canal de l'opérateur utilisé pour établir l'association au serveur Meeting Exchange.

ID d'ouverture de session* ID d'ouverture de session utilisé pour établir la connexion au serveur Meeting Exchange.

Mot de passe* Mot de passe utilisé avec l'ID d'ouverture de session pour établir la connexion au serveur Avaya Meeting Exchange.

Répertoire FTP* Répertoire FTP des fichiers audio stockés sur le pont Avaya.

Connexion FTP* Nom d'utilisateur pour la connexion FTP.

Mot de passe FTP* Mot de passe pour la connexion FTP.

Numéro de connexion Meeting Exchange* Numéro de téléphone valide composé par Connect Pro pour atteindre le serveur Meeting Exchange.

Adaptateur de téléphonie InterCall

L'adaptateur de téléphonie InterCall permet aux hôtes et présentateurs des réunions, ainsi qu'aux participants, de contrôler les fonctionnalités de conférence audio depuis les salles de réunion Connect Pro. Cet adaptateur requiert un fournisseur VoIP ou SIP, ainsi que Flash Media Gateway (Universal Voice) pour l'enregistrement des réunions. Réalisez la procédure suivante pour activer l'adaptateur de téléphonie.

Planification du déploiement

Pour le déploiement de l’adaptateur InterCall, certains ports doivent être disponibles, comme l’indique le tableau suivant :

Port	Description
80	InterCall utilise le port 80 pour communiquer avec Connect Pro sur HTTP. Ce port doit être ouvert pour la communication entrante afin de recevoir les rappels d’InterCall vers Connect Pro.
443	InterCall utilise le port 443 pour communiquer avec Connect Pro sur HTTPS (SSL). Ce port doit être ouvert pour la communication entrante afin de recevoir les rappels d’InterCall vers Connect Pro. Si vous souhaitez recevoir les rappels sécurisés à l’aide du protocole SSL, vous devez suivre des étapes de configuration supplémentaires ; pour plus d’informations, consulter la TechNote à l’adresse www.adobe.com/go/learn_cnn_customize_adaptor_fr.
8443	Connect Pro utilise le port 8443 pour communiquer avec InterCall sur HTTPS (SSL). Connect Pro utilise ce port pour CCAPI et les services d’autorisation. Ce port doit être ouvert pour que les messages sortants puissent être envoyés depuis Connect Pro à InterCall.
9080	Comme cela a été mentionné précédemment, ce port est nécessaire à la téléphonie en général. Pour InterCall, toutefois, il doit en plus être ouvert sur le pare-feu de chaque nœud d’un cluster.

Informations nécessaires à l'installation

Les éléments repérés par un astérisque (*) sont obligatoires.

Activer l’accès en cours de conférence Sélectionner cette option pour activer l'accès en cours de conférence dans l'intégralité du système. Si vous ne sélectionnez pas cette option, les sélections que vous effectuez pour les quatre entrées suivantes sont ignorées. Si vous sélectionnez cette option, utilisez les quatre options suivantes pour indiquer le mode d'implémentation de l'accès en cours de conférence.

Activer l’accès en cours de conférence pour l’hôte Sélectionner cette option pour autoriser l'accès en cours de conférence à l'hôte de la réunion.

Activer l’accès en cours de conférence pour le présentateur Sélectionner cette option pour autoriser l'accès en cours de conférence au présentateur.

Activer l’accès en cours de conférence pour le participant Sélectionner cette option pour autoriser l'accès en cours de conférence aux participants.

Activer la boîte de dialogue M’appeler Si l'accès en cours de conférence est activé, sélectionnez cette option afin d'afficher la boîte de dialogue M'appeler pour les participants lorsqu'ils rejoignent une réunion.

Hôte CCAPI* URL du service InterCall CCAPI.

Hôte d’autorisation CCAPI* URL du service d’autorisation InterCall CCAPI.

URL de rappel client* URL de rappel utilisée par le service InterCall pour rappeler Connect Pro. Cette URL doit être accessible publiquement.

Jeton d’application* Valeur utilisée pour identifier votre connexion avec le service de conférence audio InterCall.

Codes des pays* Liste des codes des pays pour lesquels Connect Pro affiche les numéros de service de conférence disponibles.

Code pays n° d’appel sans frais Code pays dans lequel le numéro de la conférence est gratuit, par exemple US.

Adaptateur de téléphonie MeetingOne

L’adaptateur de téléphonie MeetingOne permet aux hôtes et présentateurs des réunions, ainsi qu’aux participants, de contrôler les fonctionnalités de conférence audio depuis les salles de réunion Connect Pro.

Informations nécessaires à l'installation

Les éléments repérés par un astérisque (*) sont obligatoires.

Activer l'accès en cours de conférence Sélectionner cette option pour activer l'accès en cours de conférence dans l'intégralité du système. Si vous ne sélectionnez pas cette option, les sélections que vous effectuez pour les quatre entrées suivantes sont ignorées. Si vous sélectionnez cette option, utilisez les quatre options suivantes pour indiquer le mode d'implémentation de l'accès en cours de conférence.

Activer l'accès en cours de conférence pour l'hôte Sélectionner cette option pour autoriser l'accès en cours de conférence à l'hôte de la réunion.

Activer l'accès en cours de conférence pour le présentateur Sélectionner cette option pour autoriser l'accès en cours de conférence au présentateur.

Activer l'accès en cours de conférence pour le participant Sélectionner cette option pour autoriser l'accès en cours de conférence aux participants.

Activer la boîte de dialogue M'appeler Si l'accès en cours de conférence est activé, sélectionnez cette option afin d'afficher la boîte de dialogue M'appeler pour les participants lorsqu'ils rejoignent une réunion.

URL de l'API MeetingOne* URL du service API de conférence audio MeetingOne.

SSH Indique si le téléchargement SSH des enregistrements est activé.

Adaptateur de téléphonie PGi (auparavant Premiere Global) NA ou EMEA

L'adaptateur de téléphonie PGi permet aux hôtes et présentateurs des réunions, ainsi qu'aux participants, de contrôler les fonctionnalités de conférence audio depuis les salles de réunion Connect Pro. Les informations de cette section s'appliquent aux adaptateurs PGi NA et PGi EMEA.

Informations nécessaires à l'installation

Les éléments repérés par un astérisque (*) sont obligatoires.

Activer l'accès en cours de conférence Sélectionner cette option pour activer l'accès en cours de conférence dans l'intégralité du système. Si vous ne sélectionnez pas cette option, les sélections que vous effectuez pour les quatre entrées suivantes sont ignorées. Si vous sélectionnez cette option, utilisez les quatre options suivantes pour indiquer le mode d'implémentation de l'accès en cours de conférence.

Activer l'accès en cours de conférence pour l'hôte Sélectionner cette option pour autoriser l'accès en cours de conférence à l'hôte de la réunion.

Activer l'accès en cours de conférence pour le présentateur Sélectionner cette option pour autoriser l'accès en cours de conférence au présentateur.

Activer l'accès en cours de conférence pour le participant Sélectionner cette option pour autoriser l'accès en cours de conférence aux participants.

Activer la boîte de dialogue M'appeler Si l'accès en cours de conférence est activé, sélectionnez cette option afin d'afficher la boîte de dialogue M'appeler pour les participants lorsqu'ils rejoignent une réunion.

Remarque : *Les quatre valeurs suivantes vous sont fournies par PGi.*

Nom d'hôte PGi* Nom d'hôte ou adresse IP du service de conférence audio PGi. Pour l'adaptateur PGi NA, cette valeur est généralement csaxis.premconf.com. Pour l'adaptateur PGi EMEA, cette valeur est généralement euaxis.premconf.com.

Numéro de port PGi* Numéro de port que Connect Pro utilise pour se connecter au service de conférence audio PGi. Cette valeur est généralement 443.

ID Web PGi* ID que vous utilisez pour vous connecter au service de conférence audio PGi.

Mot de passe PGi* Mot de passe que vous utilisez pour vous connecter au service de conférence audio PGi.

ID ouv. sess. téléch. enregist.* ID d'ouverture de session utilisé pour télécharger les enregistrements audio du service de conférence audio PGi.

Mot de passe de téléchargement* Mot de passe utilisé avec l'ID d'ouverture de session de téléchargement des enregistrements et permettant de récupérer les enregistrements depuis le service de conférence audio PGi.

URL de téléchargement URL qu'utilise Connect Pro pour télécharger les enregistrements depuis le service de conférence audio PGi. La valeur par défaut de l'adaptateur PGi NA est https://ww5.premconf.com/audio/. La valeur par défaut de l'adaptateur PGi EMEA est http://eurecordings.premiereglobal.ie/audio/.

Chapitre 2 : Installation de Connect Pro

Après avoir examiné et réuni toutes les informations nécessaires (voir « Préparation de la migration, de l'installation et de la configuration » à la page 1), vous êtes prêt à installer Acrobat ®Connect™.

Procédure d'installation

1 si vous effectuez une migration à partir d'une version de Connect Pro antérieure à la version 7.5 :

a Suivez les étapes préalables à la migration ; voir « Préparation de la migration » à la page 5.

b Installez Connect Pro 7.5 ; voir « Installation de Connect Pro 7.5 (utilisateurs effectuant une migration uniquement) » à la page 22.

c Configurez Connect Pro 7.5 ; voir « Configuration de Connect Pro 7.5 (utilisateurs effectuant une migration uniquement) » à la page 24.

d Vérifiez l'installation de Connect Pro 7.5 ; voir « Vérification de l'installation » à la page 30.

2 Installez Connect Pro 7.5 SP1 ; voir « Installation de Connect Pro 7.5 SP1 » à la page 27.

3 Vérifiez l'installation de Connect Pro 7.5 SP1 ; voir « Vérification de l'installation » à la page 30.

4 Si vous installez Connect Pro pour la première fois et que vous avez installé Presence Server, configurez le serveur (voir « Intégration à Microsoft Live Communications Server 2005 et Microsoft Office Communications Server 2007 » à la page 65).

5 Installez Connect Pro Edge Server si vous le souhaitez ; voir « Installez Connect Pro Edge Server » à la page 32.

6 Effectuez les autres tâches de déploiement nécessaires à votre environnement ; voir « Déploiement et configuration de Connect Pro » à la page 35.

Installation de Connect Pro 7.5 (utilisateurs effectuant une migration uniquement)

Si vous effectuez la migration depuis une version antérieure de Connect Pro, réalisez les tâches suivantes pour installer, configurer et vérifier l'installation de Connect Pro 7.5. Installez ensuite Connect Pro 7.5 SP1.

***Remarque :** si vous installez Connect Pro pour la première fois ou si l'application Connect Pro 7.5 est installée, n'effectuez pas ces tâches. Voir plutôt « Installation de Connect Pro 7.5 SP1 » à la page 27.*

Exécution du programme d'installation

1 Connectez-vous à l'ordinateur en tant qu'administrateur.

2 Fermez toutes les applications.

3 Exécutez le programme d’installation de Connect Pro 7.5 depuis le DVD ou depuis le fichier que vous avez téléchargé.

- Si vous avez un DVD, insérez-le dans le lecteur. Dans l'écran de démarrage, cliquez sur le bouton Installation d'Adobe Acrobat Connect Pro Server 7.5. Si l'installation ne démarre pas automatiquement, double-cliquez sur le fichier install.exe situé à l'emplacement Connect\7.5\Disk1\InstData\VM\install.exe.
- Si vous avez un fichier obtenu par distribution électronique de logiciels (ESD), extrayez les fichiers et stockez-les sur votre disque dur, par exemple dans le répertoire C:\Connect_7_5_ESD. Double-cliquez sur le fichier install.exe dans *[répertoire_extraction]*\Connect\7.5\Disk1\InstData\VM\install.exe.

4 Sélectionnez une langue et cliquez sur OK pour continuer.

5 Dans l'écran d'introduction, cliquez sur Suivant pour continuer.

6 Parmi les produits suivants, sélectionnez ceux que vous souhaiteriez installer et cliquez sur Suivant pour continuer :

- Adobe Acrobat Connect Pro Server
- Flash Media Gateway

Remarque : *si vous n’avez pas de fournisseur de SIP/VOIP en amont, n’installez pas Flash Media Gateway. Pour plus d'informations, consultez la section « Options de conférence audio Connect Pro » à la page 16.*

7 Dans l’écran d’accord de licence qui apparaît, lisez le contrat, sélectionnez J’accepte les termes de ce contrat, puis cliquez sur Suivant.

8 Pour sélectionner l'emplacement d'installation de Connect Pro , faites l'une des actions suivantes puis cliquez sur Suivant :

- Cliquez sur Suivant pour accepter l'emplacement d'installation par défaut de Connect Pro (c:\breeze) ou cliquez sur Choisir pour sélectionner un autre emplacement.
- Si vous avez choisi un emplacement différent et que vous avez décidé d'utiliser l'emplacement par défaut à la place, cliquez sur Restaurer le dossier par défaut.
- La fenêtre de mise à jour de l'installation de Connect Pro existante apparaît. Activez la case à cocher qui confirme que vous avez bien sauvegardé votre base de données et le répertoire racine de Connect Pro.

9 Pour sélectionner l'emplacement d'installation de Flash Media Gateway, faites l'une des actions suivantes puis cliquez sur Suivant :

- Cliquez sur Suivant pour accepter l'emplacement d'installation par défaut (C:\Program Files\Adobe\Flash Media Gateway) ou cliquez sur Choisir pour sélectionner un autre emplacement.
- Si vous avez choisi un emplacement différent et que vous avez décidé d'utiliser l'emplacement par défaut à la place, cliquez sur Restaurer le dossier par défaut.
- Si Flash Media Gateway est déjà installé sur cet ordinateur, l'écran d'installation de mise à jour de la version de Flash Media Gateway existante apparaît.

10 Saisissez votre numéro de série puis cliquez sur Suivant.

Remarque : *Adobe vous a envoyé un message électronique contenant un lien vers le site de licences d'Adobe. Suivez ce lien pour récupérer votre numéro de série.*

11 Si l'écran du moteur de la base de données intégrée apparaît, faites l'une des actions suivantes :

- Si vous prévoyez d'installer une base de données sur un autre ordinateur, sélectionnez Ne pas installer le moteur de la base de données intégrée.
- Pour installer la base de données intégrée, sélectionnez Installer le moteur de la base de données intégrée à l'emplacement suivant. Pour installer à l'emplacement par défaut (c:\Program Files\Microsoft SQL Server), cliquez sur Suivant. Pour sélectionner un autre emplacement, cliquez sur Choisir.

Remarque : *si le programme d'installation détecte que Microsoft SQL Server est déjà installé sur cet ordinateur, le programme d'installation n'installe pas la base de données. Si vous migrez et que vous utilisez déjà la base de données intégrée, Connect Pro utilise la base de données existante. Cependant, parfois le programme d'installation détecte une ancienne version de SQL Server qui ne fonctionne pas avec Connect Pro. Suivez les étapes de la section « Désinstallation de Connect Pro » à la page 33 et relancez l'installation.*

12 Si vous avez installé le moteur de la base de données intégrée, saisissez un mot de passe fort et cliquez sur Suivant.

13 Dans l'écran Initialisation du service Connect Pro, effectuez l'une des opérations suivantes, puis cliquez sur Suivant :

- Sélectionnez Start Connect Pro... (recommandé).
- Sélectionnez Ne pas démarrer Connect Pro maintenant...

Si vous choisissez de démarrer Connect Pro après le redémarrage suivant, configurez Connect Pro avant de le lancer pour la première fois. Vous devez également configurer l'application avant d'installer Connect Pro 7.5 SP1. Pour ouvrir la console de gestion des applications afin de configurer Connect Pro, sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server > Configurer Connect Pro Server.

14 Si vous avez choisi de démarrer Connect Pro, un message vous signale que le service démarre.

Connect Pro 7.5 exécute quatre services Windows : Adobe Acrobat Connect Pro Service, Flash Media Server (FMS), Flash Media Administration Server et Adobe Acrobat Connect Pro Presence Server. Flash Media Gateway s'exécute comme Flash Media Gateway. Voir « Démarrage et arrêt des serveurs » à la page 103.

15 Cliquez sur Terminer pour quitter le Programme d'installation.

Si vous avez choisi de démarrer Connect Pro, l'Assistant de la Console de gestion des applications s'ouvre dans une fenêtre de navigateur pour vous guider tout au long des tâches de configuration (voir instructions ci-dessous).

Configuration de Connect Pro 7.5 (utilisateurs effectuant une migration uniquement)

Après l'installation de Connect Pro, le programme d'installation lance l'Assistant de la Console de gestion des applications. L'assistant vous guide lors de la configuration de la base de données et des paramètres du serveur, pour le téléchargement de votre fichier de licence et pour la création d'un administrateur.

Remarque : *si une autre application s'exécute sur le port 80, la Console de gestion des applications ne s'ouvre pas. Arrêtez l'application qui occupe le port 80 et rouvrez la Console de gestion des applications.*

Pour accéder à la Console de gestion des applications, choisissez Démarrer > Programmes > Adobe Acrobat Connect Pro Server > Configurer Adobe Connect Pro Enterprise Server , ou utilisez l'URL suivante : http://localhost:8510/console.

1. Lisez l'écran de bienvenue.

L'écran de bienvenue présente l'Assistant.

2. Entrez les paramètres de la base de données.

Définissez les valeurs des paramètres énumérés ci-dessous. Cliquez sur Suivant pour vous connecter à la base de données et vérifier vos paramètres.

Hôte de base de données Nom d'hôte de l'ordinateur sur lequel la base de données est installée. Si vous avez installé la base de données intégrée, la valeur est `localhost`.

Nom de la base de données Nom de la base de données. La valeur par défaut est `breeze`.

Port de base de données Port que la base de données utilise pour communiquer avec Connect Pro. La valeur par défaut est 1433.

Utilisateur de base de données Nom de l'utilisateur de la base de données. Si vous avez installé la base de données intégrée, la valeur par défaut est `sa`.

Mot de passe de l'utilisateur de base de données Mot de passe de l'utilisateur de la base de données. Si vous avez installé la base de données intégrée, définissez le mot de passe dans le programme d'installation.

3. Entrez les paramètres du serveur.

Nom du compte Nom qui identifie le compte Connect Pro, par exemple « Compte Connect Pro ».

Hôte Connect Pro Nom de domaine pleinement qualifié (FQDN) que les clients utilisent pour se connecter à Connect Pro. Par exemple, avec l'URL de compte http://connect.exemple.com, la valeur de l'hôte Connect Pro serait connect.exemple.com.

Port HTTP Port utilisé par Connect Pro pour communiquer via le protocole HTTP. La valeur par défaut est 80. Si vous entrez une autre valeur que 80, les clients doivent ajouter ce numéro de port au nom d'hôte dans l'URL lorsqu'ils accèdent au compte Connect Pro.

Mappages d'hôtes Nom correspond au nom d'hôte de l'ordinateur qui héberge Connect Pro. Nom externe correspond au nom de domaine pleinement qualifié que les clients utilisent pour se connecter à Connect Pro.

Remarque : *n'ajoutez pas de port au nom FQDN dans la zone Nom externe.*

Hôte SMTP Nom d'hôte de l'ordinateur hébergeant le serveur de messagerie SMTP.

Nom d'utilisateur SMTP Nom d'utilisateur servant à s'authentifier auprès de l'hôte SMTP. Si ce champ reste vide, Connect Pro essaie d'envoyer des messages électroniques sans authentification avec le serveur SMTP.

Mot de passe SMTP Le mot de passe du nom d'utilisateur SMTP.

Adresse de messagerie système Adresse de messagerie depuis laquelle les messages électroniques administratifs sont envoyés.

Adresse de messagerie de l'Assistance Adresse de messagerie de l'Assistance destinée aux utilisateurs de Connect Pro.

Adresse de messagerie Cci Adresse de messagerie en copie cachée à laquelle toutes les notifications destinées aux utilisateurs sont également envoyées. Cette variable autorise un suivi administratif des messages électroniques envoyés via Connect Pro sans que l'adresse de messagerie interne ne soit exposée.

Stockage partagé Volume et répertoire d'un serveur externe où le contenu est stocké, par exemple, \\volume\répertoire. Pour stocker du contenu sur plusieurs volumes, séparez-les par des points virgules (;). Avant de configurer cette fonction, consultez la section « Configuration du stockage partagé » à la page 59.

Taille du contenu mis en cache Nombre entier compris entre 1 et 100 définissant le pourcentage d'espace disque à utiliser pour stocker le contenu sur Connect Pro. Le cache pouvant grossir au-delà du pourcentage spécifié, dès lors il est préférable de choisir une valeur comprise entre 15 et 50. Si vous ne renseignez pas ce champ ou si vous entrez 0, aucun cache n'est utilisé et le contenu est copié en miroir sur Connect Pro et tous les volumes externes. Avant de configurer cette fonction, consultez la section « Configuration du stockage partagé » à la page 59.

4. Saisissez les paramètres Flash Media Gateway.

Saisissez les noms d'ordinateur et les noms externes des serveurs Flash Media Gateway. Les paramètres ne sont pas pris en compte instantanément. En cliquant sur OK pour confirmer les paramètres, il se peut que Connect Pro redémarre tous les serveurs Flash Media Gateway. Les paramètres sont envoyés à chaque serveur Flash Media Gateway dans un groupe.

Cliquez sur Ajouter pour ajouter les serveurs Flash Media Gateway. Saisissez les paramètres suivants :

Nom Le nom de l'ordinateur hébergeant Flash Media Gateway, par exemple janedoe-pc.

Nom externe Le nom de domaine complet du serveur hébergeant Flash Media Gateway, par exemple janedoe-pc.example.com.

Remarque : *n'ajoutez pas de port au nom FQDN dans la zone Nom externe.*

L'état indique si Connect Pro peut ou non se connecter au serveur Flash Media Gateway. Le serveur Flash Media Gateway peut prendre quelques secondes pour devenir actif. Un état « Actif » ne signifie pas que les paramètres SIP ont été envoyés au serveur Flash Media Gateway. Si Connect Pro ne peut pas se connecter à Flash Media Gateway, l'état est « Inactif ».

Cliquez sur Suivant et saisissez les paramètres suivants :

Nom d'utilisateur Le nom d'utilisateur du profil SIP utilisé par le serveur Flash Media Gateway pour créer des sessions SIP, par exemple sipUN1.

Mot de passe Le mot de passe du profil SIP utilisé par le serveur Flash Media Gateway pour créer des sessions SIP.

AVérification de votre installationdresse SIP L'adresse du serveur SIP pour le profil SIP utilisé par le serveur Flash Media Gateway pour créer des sessions SIP, par exemple 10.12.13.14:12345.

Hôte par défaut L'hôte par défaut du profil SIP. Ce paramètre est l'adresse du serveur SIP à utiliser si l'inscription avec le serveur SIP échoue. Ce paramètre est généralement défini sur la même adresse que l'adresse SIP.

Inscription Décidez si un serveur Flash Media Gateway doit s'inscrire sur le serveur SIP.

Port SIP Le port sur lequel le serveur Flash Media Gateway écoute des requêtes SIP, par exemple 5060.

Limite inférieure de port Le plus petit numéro de port pouvant servir aux données audio RTP. La valeur par défaut est 5000.

Limite supérieure de port Le numéro de port le plus élevé pouvant servir aux données audio RTP. La valeur par défaut est 6000.

Expiration de l'enregistrement L'intervalle, en secondes, auquel Flash Media Gateway renouvelle son enregistrement avec le serveur SIP. La valeur par défaut est 2 400 secondes (40 minutes).

5. Chargez le fichier de licence.

Pour activer Connect Pro, vous devez télécharger un fichier de licence d'Adobe et l'installer sur l'ordinateur qui héberge Connect Pro. Cliquez sur le lien pour télécharger votre fichier de licence depuis Adobe. Recherchez ensuite le fichier de licence téléchargé pour le copier dans l'installation de Connect Pro.

6. Créez un administrateur de compte.

Chaque compte Connect Pro doit disposer d'au moins un administrateur chargé d'effectuer des tâches dans l'application Web Connect Pro Central. Les comptes mis à niveau possèdent déjà un administrateur, mais vous pouvez en ajouter un autre ici.

Vérifiez votre installation.

Reportez-vous à la section « Vérification de l'installation » à la page 30. Lorsque vous avez déterminé que Connect Pro 7.5 fonctionne comme prévu, vous êtes prêt à installer Connect Pro 7.5 SP1 (voir les instructions ci-dessous).

Installation de Connect Pro 7.5 SP1

***Remarque :** si vous effectuez une migration à partir d'une version de Connect Pro antérieure à la version 7.5, installez d'abord Connect Pro 7.5 ; voir « Installation de Connect Pro 7.5 (utilisateurs effectuant une migration uniquement) » à la page 22. Installez ensuite Connect Pro 7.5 SP1.*

Exécution du programme d'installation

1 Connectez-vous à l'ordinateur en tant qu'administrateur.

2 Fermez toutes les applications.

3 Extrayez les fichiers du fichier ESD (obtenu par distribution électronique de logiciels) d'Adobe Connect 7.5 Service Pack 1 et stockez-les sur votre disque dur, par exemple dans C:\Connect_7_5_1_ESD.

4 Double-cliquez sur le fichier install.exe dans *[répertoire_extraction]*\Connect\7.5.1\Disk1\InstData\VM\install.exe.

5 Sélectionnez une langue et cliquez sur OK pour continuer.

6 Dans l'écran d'introduction, cliquez sur Suivant pour continuer.

7 Parmi les produits suivants, sélectionnez ceux que vous souhaiteriez installer et cliquez sur Suivant pour continuer :

- Adobe Acrobat Connect Pro Server
- Flash Media Gateway (Universal Voice)

***Remarque :** Flash Media Gateway nécessite un fournisseur de SIP/VOIP en amont. Pour plus d'informations, consultez la section « Options de conférence audio Connect Pro » à la page 16.*

- Adaptateur de téléphonie PGi (NA)
- Adaptateur de téléphonie PGi (EMEA)
- Adaptateur de téléphonie Avaya
- Adaptateur de téléphonie InterCall

***Remarque :** Si vous souhaitez utiliser l'adaptateur InterCall, vous devez installer Flash Media Gateway.*

- Adaptateur de téléphonie MeetingOne
- Presence Service

8 Dans l'écran d'accord de licence qui apparaît, lisez le contrat, sélectionnez J'accepte les termes de ce contrat, puis cliquez sur Suivant.

9 Pour sélectionner l'emplacement d'installation de Connect Pro , faites l'une des actions suivantes puis cliquez sur Suivant :

- Cliquez sur Suivant pour accepter l'emplacement d'installation par défaut de Connect Pro (c:\breeze) ou cliquez sur Choisir pour sélectionner un autre emplacement.
- Si vous avez choisi un emplacement différent et que vous avez décidé d'utiliser l'emplacement par défaut à la place, cliquez sur Restaurer le dossier par défaut.
- Si est déjà installé sur cet ordinateur, la fenêtre de mise à jour de l'installation apparaît. Activez la case à cocher qui confirme que vous avez bien sauvegardé votre base de données et le répertoire racine de Connect Pro.

10 Saisissez votre numéro de série puis cliquez sur Suivant.

***Remarque :** Adobe vous a envoyé un message électronique contenant un lien vers le site de licences d'Adobe. Suivez ce lien pour récupérer votre numéro de série.*

11 Transférez votre fichier de licence, puis cliquez sur Suivant.

Pour activer Connect Pro, vous devez télécharger un fichier de licence d'Adobe et l'installer sur l'ordinateur qui héberge Connect Pro. Cliquez sur le lien pour télécharger votre fichier de licence depuis Adobe. Recherchez ensuite le fichier de licence téléchargé pour le copier dans l'installation de Connect Pro.

12 Si l'écran du moteur de la base de données intégrée apparaît, faites l'une des actions suivantes :

- Si vous prévoyez d'installer une base de données sur un autre ordinateur, sélectionnez Ne pas installer le moteur de la base de données intégrée.
- Pour installer la base de données intégrée, sélectionnez Installer le moteur de la base de données intégrée à l'emplacement suivant. Pour installer à l'emplacement par défaut (c:\Program Files\Microsoft SQL Server), cliquez sur Suivant. Pour sélectionner un autre emplacement, cliquez sur Choisir.

Remarque : *si le programme d'installation détecte que Microsoft SQL Server est déjà installé sur cet ordinateur, le programme d'installation n'installe pas la base de données. Si vous migrez et que vous utilisez déjà la base de données intégrée, Connect Pro utilise la base de données existante. Cependant, parfois le programme d'installation détecte une ancienne version de SQL Server qui ne fonctionne pas avec Connect Pro. Suivez les étapes de la section «* *Désinstallation de Connect Pro* *»* *à la page 33* *et relancez l'installation.*

13 Si vous avez installé le moteur de la base de données intégrée, saisissez un mot de passe fort et confirmez-le, puis cliquez sur Suivant.

14 Définissez les valeurs des paramètres de connexion à la base de données répertoriés ci-dessous, puis cliquez sur Suivant. Les éléments marqués par un astérisque (*) sont obligatoires.

- **Hôte*** Nom d'hôte de l'ordinateur sur lequel la base de données est installée. Si vous avez installé la base de données intégrée, la valeur est `localhost`.
- **Port*** Port que la base de données utilise pour communiquer avec Connect Pro. La valeur par défaut est 1433.
- **Nom de la base de données*** Nom de la base de données. La valeur par défaut est `breeze`.
- **Utilisateur*** Nom de l'utilisateur de base de données. Si vous avez installé la base de données intégrée, la valeur par défaut est `sa`.
- **Mot de passe*** Mot de passe de l'utilisateur de la base de données. Si vous avez installé la base de données intégrée, vous avez défini le mot de passe à l'étape précédente.

15 Définissez les valeurs des paramètres réseau répertoriés ci-dessous, puis cliquez sur Suivant. Les éléments repérés par un astérisque (*) sont obligatoires.

- **Nom du compte*** Nom qui identifie le compte Connect Pro, par exemple « Compte Connect Pro ».
- **Hôte Connect Pro*** Nom de domaine pleinement qualifié (FQDN) que les clients utilisent pour se connecter à Connect Pro. Par exemple, avec l'URL de compte http://connect.exemple.com, la valeur de l'hôte Connect Pro serait connect.exemple.com (sans la partie initiale « http:// »).

16 Définissez les valeurs des paramètres de messagerie répertoriés ci-dessous, puis cliquez sur Suivant. Les éléments repérés par un astérisque (*) sont obligatoires.

- **Hôte SMTP** Nom d'hôte de l'ordinateur hébergeant le serveur de messagerie SMTP.
- **Nom d'utilisateur SMTP** Nom d'utilisateur servant à s'authentifier auprès de l'hôte SMTP. Si ce champ reste vide, Connect Pro essaie d'envoyer des messages électroniques sans authentification avec le serveur SMTP.
- **Mot de passe SMTP** Mot de passe du nom d'utilisateur SMTP.
- **Adresse de messagerie*** Adresse de messagerie à laquelle sont envoyés les messages administratifs.
- **Adresse de messagerie de l'Assistance*** Adresse de messagerie à laquelle sont envoyées les demandes d'assistance des utilisateurs de Connect Pro.

- **Adresse de messagerie Cci** Adresse de messagerie en copie cachée à laquelle toutes les notifications destinées aux utilisateurs sont également envoyées. Cette variable autorise un suivi administratif des messages électroniques envoyés via Connect Pro sans que l'adresse de messagerie interne ne soit exposée.

17 Définissez les valeurs des paramètres de stockage partagé répertoriés ci-dessous, puis cliquez sur Suivant.

- **Stockage partagé** Volume et répertoire d'un serveur externe où le contenu est stocké, par exemple, \\volume\répertoire. Pour stocker du contenu sur plusieurs volumes, séparez-les par des points virgules (;). Avant de configurer cette fonction, consultez la section « Configuration du stockage partagé » à la page 59.
- **Taille du contenu mis en cache** Nombre entier compris entre 1 et 100 définissant le pourcentage d'espace disque à utiliser pour stocker le contenu sur Connect Pro. La valeur du cache pouvant être supérieure au pourcentage spécifié, il est préférable de choisir une valeur comprise entre 15 et 50. Si vous ne renseignez pas ce champ ou si vous entrez 0, aucun cache n'est utilisé et le contenu est copié en miroir sur Connect Pro ou sur un volume externe. Avant de configurer cette fonction, consultez la section « Configuration du stockage partagé » à la page 59.

18 Si l'écran Flash Media Gateway apparaît, saisissez les paramètres suivants, puis cliquez sur Suivant. Les paramètres ne sont pas pris en compte instantanément. En cliquant sur OK pour confirmer les paramètres, il se peut que Connect Pro redémarre tous les serveurs Flash Media Gateway. Les paramètres sont envoyés à tous les serveurs Flash Media Gateway d'un cluster.

- **Nom d'utilisateur** Nom d'utilisateur du profil SIP utilisé par le serveur Flash Media Gateway pour créer des sessions SIP, par exemple sipUN1.
- **Mot de passe** Mot de passe du profil SIP utilisé par le serveur Flash Media Gateway pour créer des sessions SIP.
- **Adresse SIP** Adresse du serveur SIP pour le profil SIP utilisé par le serveur Flash Media Gateway pour créer des sessions SIP, par exemple 10.12.13.14.
- **Hôte par défaut** Hôte par défaut du profil SIP. Ce paramètre est l'adresse du serveur SIP à utiliser si l'inscription avec le serveur SIP échoue. Ce paramètre est généralement défini sur la même valeur que celle de l'adresse SIP.
- **Limite inférieure de port** Plus petit numéro de port pouvant servir aux données audio RTP. La valeur par défaut est 5000.
- **Limite supérieure de port** Plus grand numéro de port pouvant servir aux données audio RTP. La valeur par défaut est 6000.
- **Expiration de l'inscription** Intervalle, en secondes, auquel Flash Media Gateway renouvelle son enregistrement avec le serveur SIP. La valeur par défaut est 2 400 secondes (40 minutes).
- **Port SIP** Port sur lequel le serveur Flash Media Gateway écoute les requêtes SIP. La valeur par défaut est 5060.
- **Inscription** Décidez si un serveur Flash Media Gateway doit s'inscrire sur le serveur SIP.

19 Indiquez les valeurs demandées pour créer un administrateur de compte, puis cliquez sur Suivant. Les éléments repérés par un astérisque (*) sont obligatoires.

Chaque compte Connect Pro doit disposer d'au moins un administrateur chargé d'effectuer des tâches dans l'application Web Connect Pro Central. Les comptes mis à niveau possèdent déjà un administrateur, mais vous pouvez en ajouter un autre ici.

20 Indiquez les informations nécessaires concernant les adaptateurs de téléphonie que vous souhaitez installer. Pour plus d'informations sur les adaptateurs de téléphonie, voir « Choix de l'installation des adaptateurs de téléphonie intégrés » à la page 14.

Si vous ne disposez pas des informations nécessaires mais que vous souhaitez néanmoins installer l'adaptateur, sélectionnez Installer mais ne pas configurer. Lorsque vous êtes prêt à saisir les informations obligatoires, exécutez de nouveau le programme d'installation.

21 Passez en revue le résumé de pré-installation. Cliquez sur Précédent pour modifier ces paramètres. Cliquez sur Installer pour installer le logiciel.

22 Dans l'écran Initialisation du service Connect Pro, effectuez l'une des opérations suivantes, puis cliquez sur Suivant :

- Sélectionnez Start Connect Pro... (recommandé).
- Sélectionnez Ne pas démarrer Connect Pro maintenant.

23 Si vous avez choisi de démarrer Connect Pro, un message vous signale que le service démarre.

Connect Pro 7.5 SP1 exécute cinq services Windows : Adobe Acrobat Connect Pro Service, Flash Media Server (FMS), Flash Media Administration Server, Adobe Acrobat Connect Pro Telephony Service et Adobe Acrobat Connect Pro Presence Server. Flash Media Gateway s'exécute comme Flash Media Gateway. Voir « Démarrage et arrêt des serveurs » à la page 103.

24 Cliquez sur Terminer pour quitter le Programme d'installation.

25 Vérifiez votre installation.

Suivez les instructions de la section suivante afin de vérifier que votre installation de Connect Pro 7.5 SP1 est configurée correctement et qu’elle fonctionne comme prévu.

Vérification de l'installation

Effectuez les tâches suivantes pour vérifier que votre installation a été réalisée correctement et que tous les composants standard fonctionnent comme prévu. Lorsque vous êtes prêt à déployer Connect Pro, consultez « Déploiement et configuration de Connect Pro » à la page 35.

Vérification de la connectivité de la base de données

Si vous pouvez vous connecter à Connect Pro Central (application Web située dans Connect Pro), la base de données et Connect Pro peuvent fonctionner ensemble.

1 Accédez à l'adresse URL suivante : http://*[nomhôte]* .

***Remarque :** Dans cette URL, [nomhôte] correspond à la valeur définie pour Hôte Connect Pro dans l’écran Paramètres réseau du programme d’installation.*

2 Saisissez le nom d’utilisateur et le mot de passe que vous avez définis dans l’écran Connexion à la base de données du programme d’installation.

Si vous pouvez vous connecter, l'onglet d'accueil de Connect Pro Central apparaît.

Vérification du bon fonctionnement des notifications électroniques

Si vous n’avez pas saisi de valeur dans le champ Hôte SMTP du programme d’installation, Connect Pro ne peut pas envoyer de notifications électroniques. Si vous avez saisi un hôte SMTP, procédez comme suit pour vérifier que Connect Pro peut bien envoyer des notifications électroniques :

1 Dans l'onglet d'accueil de Connect Pro, cliquez sur l'onglet Administration.

2 Ouvrez l'onglet Utilisateurs et groupes.

3 Cliquez sur Nouvel utilisateur.

4 Dans la page Informations sur le nouvel utilisateur, entrez les informations requises. Voici une liste partielle des options :

Adresse de messagerie Utilisez l'adresse électronique du nouvel utilisateur. Assurez-vous que l'option Envoyer par message électronique les informations sur le nouveau compte, nom d'utilisateur et mot de passe est activée.

Nouveau mot de passe Créez un mot de passe de 4 à 16 caractères.

5 Cliquez sur Suivant pour continuer.

6 Sous l'en-tête Modifier l'appartenance à un groupe, sélectionnez un groupe, affectez l'utilisateur au groupe et cliquez sur Terminer.

7 Laissez suffisamment de temps à l'utilisateur pour vérifier sa notification électronique.

Si l'utilisateur a reçu la notification, Connect Pro fonctionne et vous pouvez envoyer des messages électroniques à l'aide du serveur de messagerie.

8 Si le message électronique n'arrive pas, procédez comme suit :

a Vérifiez la validité de l'adresse de messagerie.

b Assurez-vous que le message n'ait pas été filtré en tant que courrier indésirable.

c Assurez-vous d'avoir configuré Connect Pro avec un hôte SMTP valide et que le service SMTP fonctionne en dehors de Connect Pro.

d Contactez l'Assistance technique d'Adobe à l'adresse www.adobe.com/go/connect_licensed_programs_fr.

Vérification du bon fonctionnement d'Adobe Presenter

Pour vérifier le bon fonctionnement d'Adobe Presenter, publiez une présentation Microsoft PowerPoint sur Connect Pro pour sa compilation en présentation Flash, puis affichez-la.

1 Si vous ne l'avez pas encore fait, installez Adobe Presenter sur un ordinateur de bureau client sur lequel PowerPoint est déjà installé.

2 Lancez un navigateur et ouvrez Connect Pro Central à l'aide du nom de domaine pleinement qualifié de votre Connect Pro Server (par exemple, connect.exemple.com).

3 Cliquez sur Ressources > Prise en main.

4 Sur la page Mise en route, cliquez sur Publier des présentations > Installer Adobe Presenter.

5 Exécution du programme d'installation.

6 Si vous n'avez pas de présentation PowerPoint, créez et enregistrez une présentation constituez d'une ou deux diapositives.

7 Ouvrez l'Assistant de publication de Connect Pro en choisissant Publier dans le menu Adobe Presenter de PowerPoint.

8 Sélectionnez Connect Pro et entrez les informations sur votre serveur.

9 Connectez-vous avec votre adresse de messagerie et votre mot de passe et suivez les étapes dans l'assistant de publication. Assurez-vous de faire partie du groupe Auteurs (Administration > Utilisateurs et Groupes dans Connect Pro Central).

Lorsque vous avez terminé les étapes de l'Assistant de publication, Adobe Presenter charge votre présentation PowerPoint sur Connect Pro qui la compile en présentation Flash.

10 A la fin de la compilation, ouvrez l'onglet Contenu dans Connect Pro Central et recherchez votre présentation.

11 Ouvrez votre présentation pour l'afficher.

Vérification du bon fonctionnement du module Formation (s’il est activé)

Remarque : *Connect Pro Training est une fonctionnalité optionnelle qui doit être activée dans votre licence.*

❖ Cliquez sur l'onglet Formation de Connect Pro Central.

Si vous pouvez afficher et accéder à l'onglet Formation, Connect Training fonctionne correctement. Assurez-vous de faire partie du groupe Directeurs de formation (Administration > Utilisateurs et Groupes).

Vérification du bon fonctionnement du module Réunion (s'il est activé)

Remarque : *Connect Pro Meeting est une fonctionnalité optionnelle qui doit être activée dans votre licence.*

Pour vérifier le bon fonctionnement de Connect Pro Meeting, vous devez faire partie du groupe Hôtes de réunions ou du groupe Administrateurs.

1 Connectez-vous à Connect Pro Central en tant qu'utilisateur membre du groupe Hôtes de réunions ou Administrateurs.
2 Cliquez sur l'onglet Réunions et sélectionnez Nouvelle réunion.
3 Dans la page Entrer les informations sur la réunion, entrez les informations requises. Pour l'option Accès à la réunion, choisissez Seuls les utilisateurs inscrits et les visiteurs acceptés sont admis à la réunion. Cliquez sur Terminer pour créer la réunion.
4 Cliquez sur le bouton Entrer dans la salle de réunion.
5 Identifiez-vous pour participer à la réunion en tant qu'utilisateur inscrit.
6 Si la fenêtre Acrobat Connect Add-in apparaît, suivez les instructions pour l'installer.

Si la salle de réunion s'ouvre, Connect Pro Meeting fonctionne correctement.

Vérification du bon fonctionnement du module Evénements (s'il est activé)

Remarque : *Connect Pro Events est une fonctionnalité optionnelle qui doit être activée dans votre licence.*

1 Connectez-vous à Connect Pro Central en tant qu'utilisateur membre du groupe Gestionnaires d'événements ou Administrateurs.
2 Cliquez sur l'onglet Evénements de Connect Pro Central.

Si vous pouvez afficher et accéder à cet onglet, Connect Pro Events fonctionne correctement.

Installez Connect Pro Edge Server

Suivez les étapes ci-dessous si vous souhaitez installer Connect Pro Edge Server.

Exécution du programme d'installation

1 Fermez toutes les autres applications.
2 Accédez à l’emplacement dans lequel vous avez extrait les fichiers lors de l’installation de Connect Pro 7.5 SP1, par exemple C:\Connect_7_5_1_ESD. Double-cliquez sur le fichier edgesetup.exe stocké dans le dossier racine.
3 Sélectionnez une langue dans la boîte de dialogue prévue à cet effet. Cliquez sur OK pour continuer.

4 Dans l'écran de configuration, cliquez sur Suivant pour continuer.

5 Dans l'écran d'accord de licence qui apparaît, lisez le contrat, sélectionnez J'accepte les termes de ce contrat, puis cliquez sur Suivant.

6 Effectuez l'une des opérations suivantes :

- Cliquez sur Suivant pour accepter le répertoire d'installation par défaut (c:\breeze), ou cliquez sur Parcourir pour choisir un autre emplacement, puis cliquez sur Suivant.
- Si Connect Pro Edge Server est déjà installé sur cet ordinateur, la fenêtre de mise à jour de l'installation existante d'Adobe Acrobat Connect Pro Edge Server apparaît. Cliquez sur Suivant.

7 Dans l'écran Sélectionnez un groupe de programmes, effectuez l'une des opérations suivantes :

- Cliquez sur Suivant pour accepter l'emplacement par défaut des raccourcis du menu Démarrer.
- Cliquez sur Parcourir pour sélectionner un autre emplacement.

8 Dans la boîte de dialogue Prêt pour l'installation, vérifiez les emplacements d'installation de Connect Pro Edge Server et du dossier du menu de démarrage. Cliquez sur Précédent pour vérifier ou modifier ces paramètres, ou cliquez sur Installer.

9 Cliquez sur Terminer pour quitter l'installation de Connect Pro Edge Server.

Voir aussi

« Déploiement de Connect Pro Edge Server » à la page 39

Désinstallation des serveurs

Si vous souhaitez désinstaller les serveurs, suivez les instructions de cette section.

Désinstallation de Connect Pro

Remarque : *la désinstallation de Connect Pro ne désinstalle pas SQL Server.*

1 Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server > Désinstaller Connect Pro Server.

Important : *le dossier racine (supprimé à l'étape suivante) contient les fichiers custom.ini et config.ini, ainsi que les fichiers de contenu. Si vous souhaitez conserver le contenu, copiez ces fichiers dans un autre emplacement.*

2 Supprimez le dossier Connect Pro racine. Par défaut, l'emplacement est C:\breeze.

3 (Facultatif) Désinstallez SQL Server et, si le moteur de la base de données intégrée a été installé, supprimez les clés de registre suivantes :

Remarque : *supprimez ces clés de registre* ***après*** *avoir désinstallé SQL server, pas avant.*

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft SQL Server
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSSQLSERVER

Désinstallation de Connect Pro Edge Server

1 Sélectionnez Démarrer > Paramètres > Panneau de configuration > Ajout/Suppression de programmes > Adobe Acrobat Connect Pro Edge Server > Supprimer.

2 Supprimez le dossier Connect Pro racine. Par défaut, l'emplacement est C:\breeze.

Désinstallation de Flash Media Gateway

Flash Media Gateway est désinstallé lorsque vous désinstallez Connect Pro. Vous pouvez également exécuter le programme suivant pour désinstaller Flash Media Gateway : Program Files\Adobe\Flash Media Gateway\Uninstall_Flash Media Gateway\ Uninstall Flash Media Gateway.exe.

Chapitre 3 : Déploiement et configuration de Connect Pro

Après avoir installé Adobe®Connect™, Flash Media Gateway ou Connect Pro Edge Server et terminé la première phase de configuration avec la Console de gestion des applications, configurez l'une de ces fonctions facultatives et déployez le serveur.

Déploiement de Connect Pro

Déploiement de Connect Pro Server

1 Sur votre serveur DNS, définissez un nom de domaine pleinement qualifié pour Connect Pro (par exemple, connect.masociété.com). Mappez ce nom de domaine sur l'adresse IP statique de l'ordinateur qui héberge Connect Pro.

2 Si vous souhaitez que Connect Pro soit disponible hors de votre réseau, configurez les ports suivants dans un pare-feu :

80 Port associé par défaut au serveur d'applications Connect Pro. Port tertiaire du serveur de réunions (Flash Media Server).

1935 Port par défaut du serveur de réunions (Flash Media Server).

443 Port par défaut pour SSL. Port secondaire du serveur de réunions (Flash Media Server).

Remarque : *Si le trafic de Connect Pro passe par une passerelle (avec une adresse IP différente), assurez-vous que les pare-feu soient configurés pour accepter les requêtes provenant de l'adresse IP de cette passerelle.*

Pour obtenir de l'aide pour le déploiement de Connect Pro, contactez l'assistance technique d'Adobe à l'adresse www.adobe.com/go/connect_licensed_programs_fr.

Voir aussi

« Configuration des ports » à la page 3

Déployer un cluster de serveurs Connect Pro

Avant de déployer un cluster, les éléments suivants sont nécessaires :

- Une licence prenant en charge le nombre de nœuds que compte votre cluster. Pour plus d'informations, contactez votre représentant Adobe.
- Chaque ordinateur du cluster doit posséder une adresse IP statique et une entrée DNS.
- Un serveur de messagerie.
- Une installation SQL Server 2005 Standard Edition sur un ordinateur dédié disposant d'une adresse IP statique. Si vous installez Connect Pro dans un cluster, vous ne pouvez pas utiliser le moteur de base de données intégré. Chaque serveur hébergeant Connect Pro se connecte à la base de données, mais les restrictions liées à la licence n'autorisent la connexion que d'un seul serveur au moteur de base de données intégré.
- Une solution d'équilibrage de charge matérielle ou logicielle. Une solution d'équilibrage de charge matérielle nécessite un ordinateur distinct avec une adresse IP statique et une entrée DNS. Une solution logicielle peut être installée sur l'un des nœuds du cluster.

- Un ou plusieurs volumes de stockage partagé. Cette configuration n'est pas obligatoire, mais recommandée.

Avant de pouvoir déployer Connect Pro dans un cluster, installez-le sur un seul ordinateur. Configurez également les fonctionnalités supplémentaires (par exemple, SSL, une intégration de service d'annuaire, une authentification unique, un stockage de contenu partagé, etc.) et vérifiez qu'elles fonctionnent correctement sur ce serveur.

1 Installez et configurez Connect Pro sur un serveur dédié.

Utilisez les mêmes numéro de série et fichier de licence pour chaque installation de Connect Pro. N'installez pas le moteur de base de données intégré et, si votre solution de stockage partagé requiert la saisie d'un nom d'utilisateur et d'un mot de passe, ne démarrez pas Connect Pro à partir du programme d'installation.

2 Si votre solution de stockage partagé requiert la saisie d’un nom d’utilisateur et d’un mot de passe, procédez comme suit pour les ajouter à Connect Pro Service :

a Ouvrez le panneau de configuration Services.

b Double-cliquez sur Adobe Acrobat Connect Pro Service.

c Cliquez sur l'onglet Connexion.

d Cliquez sur la case d'option Ce compte et entrez le nom d'utilisateur du stockage partagé dans le champ. La syntaxe du nom d'utilisateur est [sous-domaine\]nom d'utilisateur.

e Entrez et confirmez le mot de passe du stockage partagé.

f Cliquez sur Appliquer, puis sur OK.

3 Procédez comme suit pour démarrer Connect Pro :

a Dans le panneau de configuration Services, sélectionnez Flash Media Server (FMS) et cliquez ensuite sur Démarrer le service.

b Dans le panneau de configuration Services, sélectionnez Adobe Acrobat Connect Pro Service et cliquez ensuite sur Démarrer le service.

4 Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server > Configurer Connect Pro Server pour ouvrir la Console de gestion des applications. Cliquez sur Suivant.

5 Dans l'écran Paramètres de la base de données, entrez les informations relatives à la base de données SQL Server, puis cliquez sur Suivant.

Si Connect Pro est parvenu à se connecter à la base de données, un message de confirmation s'affiche et la fenêtre Paramètres de la base de données s'ouvre. Cliquez sur Suivant.

6 Dans l'écran Paramètres du serveur, procédez comme suit et cliquez sur Suivant :

a Entrez un nom de compte.

b Dans le champ Hôte Connect Pro, entrez le nom de l'ordinateur qui exécute l'équilibreur de charge.

c Entrez un numéro de port HTTP. Ce numéro peut être 80 ou 8080 selon l'équilibreur de charge utilisé.

d Entrez le nom externe du nœud de cluster.

e Entrez le nom de domaine de l'hôte SMTP et du système, ainsi que les adresses électroniques d'assistance.

f Si vous utilisez un stockage partagé, entrez le chemin d'accès au(x) volume(s) (séparez les volumes à l'aide d'un point-virgule).

g Entrez le pourcentage du serveur Connect Pro que vous souhaitez utiliser comme cache local.

Remarque : *le contenu est écrit dans le cache local et le volume de stockage partagé. Le contenu est conservé dans le cache local pendant 24 heures après sa dernière utilisation. Si le pourcentage de cache a été dépassé a l'issue de cette période, le contenu est vidé.*

7 Transférez le fichier de licence, puis cliquez sur Suivant.

8 Créez un administrateur et cliquez sur Terminer.

9 Répétez les étapes 1 à 8 pour chaque serveur du cluster.

10 Pour configurer l'équilibreur de charge, procédez comme suit :

a Configurez l'équilibreur de charge de sorte qu'il écoute sur le port 80.

b Ajoutez tous les noms des nœuds de cluster au fichier de configuration de l'équilibreur de charge.

***Remarque :** pour plus d'informations sur la configuration de l'équilibreur de charge, consultez la documentation du fabricant.*

11 Ouvrez un navigateur Web et entrez le nom de domaine de l’équilibreur de charge ; par exemple, http://connect.masociété.com.

Pour obtenir de l'aide sur le déploiement d'un cluster, contactez l'assistance technique d'Adobe à l'adresse www.adobe.com/go/connect_licensed_programs_fr.

Voir aussi

« Installation de Connect Pro 7.5 SP1 » à la page 27

« Configuration du stockage partagé » à la page 59

Vérification des opérations au sein d'un cluster

Si un ordinateur d'un cluster s'arrête, l'équilibreur de charge achemine toutes les requêtes HTTP vers un ordinateur opérationnel du cluster.

Lorsqu'une réunion commence, le serveur d'applications affecte un hôte principal et un hôte de secours à la salle de réunion en fonction de la charge rencontrée. Lorsque l'hôte principal s'arrête, les clients se reconnectent à l'hôte de secours.

Il est préférable de vérifier que le contenu chargé sur un serveur d'un cluster est bien répliqué sur les autres ordinateurs du cluster.

Dans les procédures suivantes, le cluster contient deux ordinateurs : Ordinateur1 et Ordinateur2.

Vérification de l'équilibrage de charge et du basculement de réunion

1 Démarrez Connect Pro sur les deux ordinateurs.

a Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server > Démarrer Connect Pro Meeting Server.

b Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server > Démarrer Connect Pro Central Application Server.

2 Connectez-vous à Connect Pro Central à partir de l'URL suivante :

http://*[nomhôte]*

Pour *nomhôte*, utilisez la valeur Hôte Connect Pro que vous avez saisie dans la Console de gestion des applications.

3 Sélectionnez l'onglet Réunions et cliquez sur le lien d'une réunion pour accéder à une salle de réunion.

Au besoin, créez une nouvelle réunion.

4 Arrêtez Connect Pro sur Ordinateur2.

a Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server > Arrêter·Connect Pro Central Application Server.

b Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server > Arrêter Connect Pro Meeting Server.

Si le basculement de réunion a bien fonctionné, le témoin de connexion de la réunion doit toujours être vert.

5 Dans Connect Pro Central, cliquez sur un onglet ou un lien quelconque.

Si l'équilibreur de charge fonctionne, vous devriez encore être en mesure d'envoyer des requêtes à Connect Pro Central et de recevoir des réponses.

Si le cluster contient plusieurs ordinateurs, testez cette procédure de démarrage-arrêt sur chacun d'eux.

Vérification de la réplication de contenu

1 Démarrez Connect Pro sur Ordinateur1.

a Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server > Démarrer Connect Pro Meeting Server.

b Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server > Démarrer Connect Pro Central Application Server.

2 Arrêtez Connect Pro sur Ordinateur2.

a Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server > Arrêter·Connect Pro Central Application Server.

b Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server > Arrêter Connect Pro Meeting Server.

3 Connectez-vous à Connect Pro Central à partir de l'URL suivante :

http://*[nomhôte]*

Pour *nomhôte*, entrez la valeur Hôte Connect Pro que vous avez saisie dans la Console de gestion des applications.

4 Transférez une image JPEG ou un autre contenu vers Connect Pro sur Ordinateur1 :

- Pour ce faire, vous devez être membre du groupe Auteurs. (Si vous êtes Administrateur de compte, vous pouvez vous ajouter vous-même au groupe Auteurs dans Connect Pro Central.)
- Cliquez sur l'onglet Contenu.
- Cliquez sur Nouveau contenu et suivez les instructions qui s'affichent dans votre navigateur pour ajouter du contenu.

Lorsque le transfert de votre contenu test est terminé, la page Contenu utilisateurs s'ouvre et présente la liste des fichiers qui vous appartenaient.

5 Cliquez sur le lien pointant vers le contenu test que vous venez de transférer.

Une page d'informations sur les contenus contenant l'adresse URL qui permet d'afficher ce contenu apparaît.

6 Notez l'adresse URL pour l'utiliser à l'étape 10.

7 Cliquez sur l'URL.

8 Démarrez Ordinateur2, attendez que le démarrage de Connect Pro soit terminé, puis arrêtez Ordinateur1.

Si vous avez configuré un périphérique de stockage externe, il n'est pas nécessaire d'attendre que Ordinateur2 s'arrête ; le contenu requis est copié à partir du périphérique externe.

9 Fermez la fenêtre du navigateur dans laquelle le contenu test est affiché.

10 Ouvrez une nouvelle fenêtre de navigateur et entrez l'URL permettant d'afficher votre contenu test.

Si ce contenu apparaît, la réplication vers Ordinateur2 fonctionne. Une fenêtre vide ou un message d'erreur signifie que la réplication n'a pas fonctionné.

Déploiement de Connect Pro Edge Server

Procédure d'installation de Connect Pro Edge Server

1. Créez les régions des serveurs Edge.

Vous pouvez configurer des serveurs Edge ou des clusters de serveurs Edge dans différents sites, ou *régions*, afin d'affecter et d'équilibrer l'accès à Connect Pro. Par exemple, vous pouvez configurer un serveur Edge à San Francisco pour les utilisateurs de la côte ouest des Etats-unis et un autre serveur Edge à Boston pour ceux de la côte est.

2. Installez Connect Pro Edge Server.

Installez Connect Pro Edge Server sur chaque ordinateur de chaque région. Par exemple, si vous avez un cluster de serveurs Edge dans une région, installez Connect Pro Edge Server sur chaque ordinateur du cluster. Reportez-vous à la section « Installez Connect Pro Edge Server » à la page 32.

3. Modifiez le serveur DNS de chaque région.

Mappez le nom de domaine pleinement qualifié (FQDN) du serveur Connect Pro d'origine sur l'adresse IP statique du serveur Connect Pro Edge de chaque région. Voir la section « Déploiement de Connect Pro Edge Server » à la page 39.

4. Configurez le serveur Edge.

Vous devez ajouter les paramètres de configuration dans le fichier custom.ini de chaque serveur Connect Pro Edge. Voir la section « Déploiement de Connect Pro Edge Server » à la page 39.

5. Configurez le serveur d'origine.

Vous devez ajouter les paramètres de configuration dans le fichier custom.ini de chaque serveur Connect Pro. Vous devez également définir le Nom externe du serveur Edge dans la Console de gestion des applications du serveur d'origine. Voir la section « Déploiement de Connect Pro Edge Server » à la page 39.

6. Configurez l'équilibreur de charge.

Si vous configurez plusieurs serveurs Edge dans une région, vous devez utiliser un équilibreur pour équilibrer la charge entre les serveurs Edge et les configurer pour qu'ils écoutent le port 80. Les serveurs Edge écoutent le port 8080. Pour plus d'informations, consultez la documentation fournie par le fabricant de l'équilibreur de charge.

Déploiement de Connect Pro Edge Server

Avant de déployer des serveurs Edge, il est préférable de vérifier le bon fonctionnement de Connect Pro et de toute fonctionnalité supplémentaire (par exemple, SSL, l'intégration de services d'annuaire, l'authentification unique, le stockage de contenu partagé, etc.).

1 Dans votre serveur DNS, mappez le nom de domaine pleinement qualifié (FQDN) du serveur d'origine avec l'adresse IP statique du serveur Edge. Si vous installez des serveurs Edge dans plusieurs régions, répétez cette étape pour chacune d'elles.

Remarque : *vous pouvez également utiliser un fichier d'hôtes. Dans ce cas, chaque client doit disposer d'un fichier d'hôtes dont l'adresse IP statique du serveur Edge pointe sur le nom de domaine pleinement qualifié du serveur d'origine.*

2 Sur Connect Pro Edge Server, ouvrez le fichier *[rép_install_racine]*\edgeserver\win32\conf\HttpCache.xml et remplacez le nom de l'ordinateur indiqué dans la balise HostName par le nom de domaine pleinement qualifié (FQDN) du serveur Edge, edge1.masociété.com par exemple.

```
<!-- The real name of this host. -->
<HostName>edge1.yourcompany.com</HostName>
```

3 Dans Connect Pro Edge Server, créez un nouveau fichier *[rép_install_racine]*\edgeserver\custom.ini et saisissez les valeurs et paramètres suivants :

FCS_EDGE_HOST Nom de domaine pleinement qualifié du serveur Edge, par exemple, `FCS_EDGE_HOST=edge1.yourcompany.com`.

FCS_EDGE_REGISTER_HOST Nom de domaine pleinement qualifié (FQDN) du serveur d'origine Connect Pro ; par exemple, `FCS_EDGE_REGISTER_HOST=connect.yourcompany.com`.

FCS_EDGE_CLUSTER_ID Nom du cluster. Chaque cluster de serveurs Edge doit disposer d'un ID unique. Chaque ordinateur du cluster doit avoir le même identifiant. Le format recommandé est *`nomsociété-nomcluster`* ; par exemple, `FCS_EDGE_CLUSTER_ID=votresociété-us`.

Remarque : *vous devez configurer ce paramètre même si vous ne déployez qu'un seul serveur Connect Pro Edge.*

FCS.HTTPCACHE_BREEZE_SERVER_NORMAL_PORT Adresse IP ou nom de domaine et numéro de port de l'ordinateur sur lequel est installé Connect Pro ; par exemple, `FCS.HTTPCACHE_BREEZE_SERVER_NORMAL_PORT=connect.yourcompany.com:80`. Connect Pro Edge Server se connecte au serveur d'origine Connect Pro à cet emplacement.

FCS_EDGE_PASSWORD (Facultatif) Mot de passe du serveur Edge. Si vous définissez une valeur pour ce paramètre, vous devez définir la même valeur pour chaque serveur Edge et pour le serveur d'origine.

FCS_EDGE_EXPIRY_TIME (Facultatif) Nombre de millisecondes accordées au serveur Edge pour s'enregistrer sur le serveur d'origine avant son expiration dans le cluster et le basculement du système sur un autre serveur Edge. Commencez par la valeur par défaut `FCS_EDGE_EXPIRY_TIME=60000`.

FCS_EDGE_REG_INTERVAL (Facultatif) Intervalle, en millisecondes, durant lequel le serveur Edge tente de s'enregistrer auprès du serveur d'origine. Ce paramètre détermine la fréquence à laquelle le serveur Edge se met à la disposition du serveur d'origine. Commencez par la valeur par défaut `FCS_EDGE_REG_INTERVAL=30000`.

DEFAULT_FCS_HOSTPORT (Facultatif) Pour configurer les ports du serveur Edge, ajoutez la ligne suivante :

```
DEFAULT_FCS_HOSTPORT=:1935,80,-443
```

Le signe moins (-) placé devant 443 désigne le port 443 comme port sécurisé recevant uniquement des connexions RTMPS. Si vous tentez une demande de connexion RTMPS au port 1935 ou 80, la connexion échouera. De même, une demande de connexion RTMP non sécurisée envoyée au port 443 échoue également.

Remarque : *si votre serveur Edge utilise un accélérateur matériel externe, il n'est pas nécessaire de configurer le port 443 comme port sécurisé.*

Vous trouverez, ci-dessous, des exemples de valeurs pour le fichier config.ini :

```
FCS_EDGE_HOST=edge.yourcompany.com
FCS_EDGE_REGISTER_HOST=connect.yourcompany.com
FCS_EDGE_CLUSTER_ID=yourcompany-us
FCS.HTTPCACHE_BREEZE_SERVER_NORMAL_PORT=connect.yourcompany.com:80
```

4 Redémarrez le serveur Edge.

5 Sur le serveur d'origine Connect Pro, ouvrez le fichier *[rép_install_racine]* \custom.ini dans un éditeur de texte et mappez la valeur du paramètre `FCS_EDGE_CLUSTER_ID` sur un ID de région ; la syntaxe est `edge.`*`FCS_EDGE_CLUSTER_ID = zone-id`*. Même si vous ne déployez qu'un seul serveur Edge, vous devez mapper l'identifiant du cluster sur un identifiant de région.

Chaque cluster de serveurs Edge doit disposer d'un identifiant de région. L'identifiant de région peut être tout entier positif supérieur à 0. Par exemple, vous pouvez avoir trois clusters mappés sur les régions 1 à 3 :

```
edge.yourcompany-us=1
edge.yourcompany-apac=2
edge.yourcompany-emea=3
```

Ce qui suit est un exemple de fichier custom.ini pour le serveur d'origine :

```
DB_HOST=localhost
DB_PORT=1433
DB_NAME=breeze
DB_USER=sa
DB_PASSWORD=#V1#4cUsRJ6oeFwZLnQPpS4f0w==
# DEBUG LOGGING SETTINGS
HTTP_TRACE=yes
DB_LOG_ALL_QUERIES=yes
# EDGE SERVER SETTINGS
edge.yourcompany-us=1
```

Remarque : *si vous définissez un paramètre* `FCS_EDGE_PASSWORD` *dans le fichier config.ini du serveur Edge, définissez le même mot de passe dans le fichier custom.ini du serveur d'origine.*

6 Redémarrez le serveur d'origine.

7 Sur le serveur d'origine, ouvrez la Console de gestion des applications (Démarrer > Programmes > Adobe Acrobat Connect Pro Server > Configurer Connect Pro Server). Ouvrez l'onglet Paramètres de l'application, puis choisissez Paramètres du serveur et, dans la section Mappages de l'hôte, entrez le Nom externe du serveur Edge. Le nom externe doit être identique à la valeur définie pour le paramètre `FCS_EDGE_HOST` sur le serveur Edge.

8 Sur le serveur d'origine, configurez le pare-feu Windows de sorte que les serveurs Edge puissent accéder au port 8506.

9 Répétez les étapes 2 à 4 pour chaque serveur Edge de chaque région.

10 Répétez les étapes 5 à 7 pour chaque serveur d'origine de chaque région.

Pour obtenir de l'aide sur le déploiement des serveurs Edge, contactez l'assistance technique d'Adobe à l'adresse www.adobe.com/go/connect_licensed_programs_fr..

Voir aussi

« Choix du déploiement de Connect Pro Edge Server » à la page 14

Intégration dans un service d'annuaire

Présentation de l'intégration du service d'annuaire

Vous pouvez intégrer Connect Pro à un service d'annuaire afin d'authentifier les utilisateurs par rapport à l'annuaire LDAP et d'éviter d'ajouter manuellement des groupes et des utilisateurs individuels. Les comptes d'utilisateur sont créés automatiquement dans Connect Pro par le biais de synchronisations manuelles ou planifiées avec l'annuaire de la société.

Pour être intégré à Connect Pro, votre serveur d'annuaire doit utiliser le protocole LDAP (Lightweight Directory Access Protocol) ou LDAPS (secure Lightweight Directory Access Protocol). Le protocole LDAP est un protocole Internet client-serveur qui permet de rechercher les coordonnées des utilisateurs dans un serveur d'annuaire compatible LDAP.

Connect Pro se connecte à un annuaire LDAP en tant que client LDAP. Il importe les utilisateurs et les groupes et synchronise les informations de ceux-ci avec un annuaire LDAP. Vous pouvez également configurer Connect Pro pour authentifier les utilisateurs par rapport à l'annuaire LDAP.

Tout service d'annuaire compatible LDAP peut s'intégrer à Connect Pro. Vous trouverez la liste des annuaires LDAP certifiés à l'adresse www.adobe.com/go/connect_sysreqs_fr.

Présentation de la structure d'annuaire LDAP

Les annuaires LDAP organisent les informations selon la norme X.500.

Dans un annuaire LDAP, un utilisateur ou un groupe est appelé une *entrée*. Une entrée est un ensemble d'attributs. Un attribut se compose d'un type et d'une ou plusieurs valeurs. Les types utilisent des chaînes mnémoniques comme « `ou` »pour une entité organisationnelle ou « `cn` » pour un nom commun. Les valeurs des attributs sont des informations, telles qu'un numéro de téléphone, une adresse de messagerie et une photo. Pour connaître la structure d'annuaire LDAP de votre société, contactez votre administrateur LDAP.

Chaque entrée présente un *nom unique* qui décrit le chemin de l'entrée par l'intermédiaire d'une structure en arborescence allant de l'entrée jusqu'à la racine. Le nom unique d'une entrée dans l'annuaire LDAP est une concaténation du nom de l'entrée (appelé *nom unique relatif*, RDN) et des noms de ses entrées parentes dans la structure d'arborescence.

L'arborescence peut refléter des emplacements géographiques ou les limites des services d'une société. Par exemple, si Alicia Solis est un utilisateur du service QA d'Acme, Inc. en France, le nom unique de cet utilisateur peut être :

cn=Alicia Solis, ou=QA, c=France, dc=Acme, dc=com

Importation des branches d'annuaire

Lors de l'importation d'utilisateurs et de groupes depuis un annuaire LDAP vers Connect Pro, vous indiquez le chemin vers une section de l'arborescence LDAP à l'aide du nom unique de cette section. L'opération spécifie l'étendue de la recherche. Par exemple, vous pouvez n'importer que les utilisateurs d'un groupe particulier de votre société. Pour ce faire, vous devez savoir où sont situées les entrées de ce groupe dans l'arborescence de l'annuaire.

Une technique courante consiste à utiliser le domaine Internet de la société en tant que racine de l'arborescence. Par exemple, Acme, Inc. pourrait utiliser `dc=com` pour spécifier l'élément racine de l'arborescence. Un nom unique qui spécifie le bureau d'Acme, Inc. à Singapour pourrait être `ou=Singapour , ou=Marketing , ou=Employés , dc=Acme , dc=com`. (Dans cet exemple, « `ou` » est l'abréviation de « entité organisationnelle » et « `dc` »l'abréviation de « composant de domaine ».)

Remarque : *tous les annuaires LDAP n'ont pas de racine unique. Dans ce cas, vous pouvez importer des branches distinctes.*

Importation d'utilisateurs et de groupes

Il existe deux moyens de structurer les entrées d'utilisateurs et de groupes dans un annuaire LDAP : sous le même nœud d'une branche ou sous des branches différentes.

Si les utilisateurs et les groupes sont sous le même nœud d'une branche LDAP, les paramètres d'utilisateurs et de groupes liés à l'importation des entrées contiennent le même nom unique de branche. Cela signifie que vous devez utiliser un filtre pour ne sélectionner que les utilisateurs lorsque vous importez des utilisateurs, et un filtre pour ne sélectionner que les groupes lorsque vous importez des groupes.

Si les utilisateurs et les groupes sont placés sous des branches différentes de l'arborescence, utilisez un nom unique de branche qui sélectionne la branche d'utilisateurs lorsque vous importez les utilisateurs et la branche de groupes lorsque vous importez les groupes.

Vous pouvez également importer des sous-branches pour importer les utilisateurs de toutes les branches au-dessous d'un certain niveau. Par exemple, pour importer tous les employés du service commercial, vous pouvez utiliser le nom unique de la branche suivante :

```
ou=Sales, dc=Acme, dc=com
```

Le personnel commercial peut, cependant, être stocké dans des sous-branches. Dans ce cas, dans l'écran Mappage du profil utilisateur, définissez le paramètre Recherche de sous-arborescence sur « `true` » pour vous assurer que les utilisateurs sont importés depuis les sous-branches situées sous ce niveau dans l'arborescence.

Filtrage des entrées sélectionnées

Un filtre précise la condition que doit remplir une entrée pour être sélectionnée. Les sélections d'entrée au sein d'une partie de l'arborescence sont ainsi limitées. Par exemple, si le filtre spécifie `(objectClass=organizationalPerson)`, seules les entrées dont l'attribut est `organizationalPerson` sont sélectionnées pour l'importation.

Remarque : *l'attribut* `objectClass` *doit être présent dans toutes les entrées d'un annuaire LDAP.*

Utilisateurs et groupes internes et externes

Les utilisateurs et les groupes créés directement dans Connect Pro et non importés depuis un annuaire LDAP sont appelés utilisateurs et groupes *internes*. Les utilisateurs et les groupes importés dans la base de données Connect Pro depuis un annuaire LDAP sont appelés utilisateurs et groupes *externes*.

Pour que les groupes importés restent synchronisés avec l'annuaire LDAP externe, vous ne pouvez pas ajouter d'utilisateurs et de groupes internes dans les groupes externes. Vous pouvez, en revanche, ajouter des utilisateurs et des groupes externes dans les groupes internes.

Si la valeur de l'identifiant ou du nom d'une entrée de groupe ou d'utilisateur importée correspond à celle d'un groupe ou d'un utilisateur interne existant, la synchronisation des annuaires transforme le groupe ou l'utilisateur importé d'interne en externe et place un avertissement dans le journal de synchronisation.

Intégration de Connect Pro à un annuaire LDAP

L'intégration du service d'annuaire a lieu dans l'onglet Paramètres du service d'annuaire de la Console de gestion des applications. Utilisez un compte d'administrateur.

Vous pouvez configurer un serveur d'annuaire pour l'authentification des utilisateurs et la synchronisation LDAP. La configuration peut pointer vers une ou plusieurs branches du service d'annuaire.

1. Ouvrez la Console de gestion des applications.

Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server > Configurer Connect Pro Server.

2. Entrez les paramètres de connexion du serveur LDAP.

Ouvrez l'onglet Paramètres du service d'annuaire. Entrez des valeurs dans l'écran Paramètres LDAP > Paramètres de connexion, puis cliquez sur Enregistrer.

Lorsque vous cliquez sur Enregistrer, Connect Pro teste la connexion LDAP. Si le test échoue, le message suivant s'affiche : « Vos paramètres ont bien été enregistrés, mais la connectivité LDAP n'a pu être vérifiée. » Vérifiez l'URL et le port LDAP.

Champ	Valeur par défaut	Description
Adresse URL du serveur LDAP	Aucune valeur par défaut.	La forme habituelle est `ldap://` ***[nomduserveur:numérodeport]*** . Si votre société utilise un serveur LDAP sécurisé, utilisez `ldaps://`. Si vous ne spécifiez pas de port, Connect Pro utilise le port LDAP standard (389) ou le port LDAPS (636). Le protocole LDAPS requiert des certificats SSL. Si vous configurez Connect Pro pour travailler dans une forêt Microsoft Active Directory où le catalogue global est activé, utilisez ce dernier (port standard : 3268).
Méthode d'authentification de connexion LDAP	Aucune valeur par défaut.	Mécanisme d'authentification des informations d'identification de connexion (nom d'utilisateur LDAP, mot de passe LDAP) du compte de service LDAP pour Connect Pro (droits d'administrateur). **Simple** (authentification standard - recommandée). **Anonyme** (sans mot de passe - votre serveur LDAP doit être configuré pour autoriser la connexion anonyme). **Résumé MD5** (configurez votre serveur LDAP pour autoriser l'authentification résumée).
Nom d'utilisateur de connexion LDAP	Aucune valeur par défaut.	Identifiant de connexion d'administrateur sur le serveur LDAP.
Mot de passe de connexion LDAP	Aucune valeur par défaut.	Mot de passe d'administrateur sur le serveur LDAP.
Expiration de la requête LDAP	Aucune valeur par défaut.	Délai pouvant s'écouler avant que la requête ne soit annulée, en secondes. Si vous ne renseignez pas ce champ, il n'y a pas de délai. Définissez cette valeur sur 120.
Limite de taille de la page de requête d'entrée LDAP	Aucune valeur par défaut.	Taille de la page de résultats renvoyée par le serveur LDAP. Si ce champ est vide ou égal à 0, aucune taille de page n'est utilisée. Utilisez ce champ lorsqu'une taille de résultats maximale a été configurée pour les serveurs LDAP. Définissez une taille de page inférieure à la taille de résultats maximale de sorte que l'ensemble des résultats soit récupéré sur le serveur en plusieurs pages. Ainsi, si vous tentez d'intégrer un important annuaire LDAP qui ne peut afficher que 1 000 utilisateurs alors qu'il y en a 2 000 à importer, l'intégration échoue. Si vous définissez la taille de la page de requête sur 100, les résultats sont renvoyés sur 20 pages et tous les utilisateurs sont importés.

Voici un exemple de syntaxe LDAP pour les paramètres de connexion :

```
URL:ldap://ldapserver.mycompany.com:389
UserName:MYCOMPANY\jdoe
Password:password123
Query timeout:120
Authentication mechanism:Simple
Query page size:100
```

3. Mappez les profils utilisateurs de l'annuaire LDAP avec Connect Pro.

Ouvrez l'onglet Mappage du profil utilisateur, entrez les valeurs, puis cliquez sur Enregistrer.

Champ	Valeur par défaut	Description
Nom de connexion	Aucune valeur par défaut.	Attribut de connexion dans le service d'annuaire.
Prénom	Aucune valeur par défaut.	Attribut du prénom dans le service d'annuaire.
Nom	Aucune valeur par défaut.	Attribut du nom dans le service d'annuaire.
Adresse de messagerie	Aucune valeur par défaut.	Attribut d'adresse de messagerie dans le service d'annuaire.

Si vous avez défini des champs personnalisés, ils apparaissent dans la fenêtre Mappage du profil utilisateur. Cet exemple mappe un profil d'utilisateur Connect Pro sur un profil d'utilisateur LDAP Active Directory. Connexion réseau est un champ personnalisé.

```
Login:mail
FirstName:givenName
LastName:sn
Email:userPrincipalName
NetworkLogin:mail
```

4. (Facultatif) Ajoutez une branche d'utilisateur.

Cliquez sur Ajouter pour ajouter des informations sur un utilisateur d'une branche donnée de votre société. Entrez les valeurs dans les champs Branche et Filtre, puis cliquez sur Enregistrer.

Pour importer des utilisateurs à partir de sous-branches, sélectionnez True dans le menu Recherche de sous-arborescence, sinon sélectionnez False.

Pour plus d'informations, consultez la section « Présentation de la structure d'annuaire LDAP » à la page 42.

Champ	Valeur par défaut	Attribut/notes LDAP
Nom unique de la branche	Aucune valeur par défaut.	Nom unique du nœud racine de la branche. Un lien vers la branche sélectionnée s'affiche.
Filtre	Aucune valeur par défaut.	Chaîne du filtre de requête.
Recherche de sous-arborescence	True	True ou False. La valeur True déclenche une recherche récursive dans toutes les sous-arborescences de la branche.

5. Mappez les profils de groupes de l'annuaire LDAP avec Connect Pro.

Ouvrez l'onglet Mappage du profil de groupe, entrez des valeurs, puis cliquez sur Enregistrer.

Remarque : *Les profils de groupe Connect Pro ne prennent pas en charge les champs personnalisés.*

Champ	Valeur par défaut	Attribut/notes LDAP
Nom du groupe	Aucune valeur par défaut.	Attribut du nom du groupe dans le service d'annuaire.
Membre du groupe	Aucune valeur par défaut.	Attribut du membre du groupe dans le service d'annuaire.

Voici un mappage entre les attributs d'entrée de groupes LDAP et un profil de groupe Connect Pro :

```
Name:cn
Membership:member
```

6. (Facultatif) Ajoutez une branche de groupe.

Cliquez sur Ajouter pour ajouter des informations sur un groupe d'une branche donnée de votre société. Entrez les valeurs dans les champs Branche et Filtre, puis cliquez sur Enregistrer.

Pour importer des groupes à partir de sous-branches, sélectionnez True dans le menu Recherche de sous-arborescence, sinon sélectionnez False.

Pour plus d'informations, consultez la section « Présentation de la structure d'annuaire LDAP » à la page 42.

Champ	Valeur par défaut	Attribut/notes LDAP
Nom unique de la branche	Aucune valeur par défaut.	Nom unique du nœud racine de la branche. Chaque branche de la société possède son propre attribut de nom unique LDAP. Un lien vers la branche sélectionnée s'affiche.
Filtre	Aucune valeur par défaut.	Chaîne du filtre de requête.
Recherche de sous-arborescence	True	Valeur booléenne `true` ou `false`. La valeur `true` lance une recherche récursive dans toutes les sous-arborescences de la branche.

L'exemple suivant indique une syntaxe LDAP illustrant comment ajouter une branche de la société et définir ses groupes :

```
DN:cn=USERS,DC=myteam,DC=mycompany,DC=com
Filter:(objectClass=group)
Subtree search:True
```

7. Entrez les paramètres d'authentification.

Sélectionnez l'onglet Paramètres d'authentification. Pour authentifier les utilisateurs Connect Pro à l'aide du service d'annuaire de votre société, sélectionnez « Activer l'authentification de l'annuaire LDAP ». Si vous ne sélectionnez pas cette option, Connect Pro utilise l'authentification native (informations de connexion de l'utilisateur stockées dans la base de données Connect Pro).

Si vous activez la case à cocher « Activer la reprise de Connect Pro en cas d'échec d'authentification de l'annuaire LDAP », Connect Pro utilise l'authentification native.

Remarque : *cette option peut être utile en cas de panne de connexion LDAP momentanée sur le réseau. Il se peut, toutefois, que les informations de connexion LDAP soient différentes des celles de la base de données Connect Pro.*

Activez la case à cocher « Créer un compte d'utilisateur Connect Pro en cas d'authentification réussie à l'annuaire LDAP » pour permettre aux nouveaux utilisateurs d'accéder au serveur Connect Pro si l'authentification LDAP a réussi. Si un utilisateur de votre service d'annuaire est autorisé à utiliser Connect Pro, laissez cette option cochée et sélectionnez « Interne » comme type de compte d'utilisateur. Pour plus d'informations, consultez la section « Utilisateurs et groupes internes et externes » à la page 43.

Activez la case à cocher « Activer l'inscription de groupe lors de la connexion initiale uniquement » pour créer un identifiant dans Connect Pro et placer les utilisateurs dans des groupes spécifiques lorsqu'ils se connectent à Connect Pro pour la première fois. Entrez les groupes dans la zone Noms des groupes.

8. Planifiez la synchronisation.

Ouvrez l'onglet Paramètres de synchronisation. Dans l'écran Paramètres de planification, cochez la case Activer la synchronisation planifiée pour programmer des synchronisations régulières, quotidiennes, hebdomadaires ou mensuelles, à une heure donnée. Pour plus d'informations, consultez la section « Recommandations relatives à la synchronisation » à la page 47.

Vous pouvez également effectuer une synchronisation manuelle dans la fenêtre Actions de synchronisation.

9. Définissez une stratégie de mot de passe et une stratégie de suppression.

Ouvrez l'onglet Paramètres de la stratégie, choisissez une stratégie de configuration des mots de passe et une stratégie de suppression, puis cliquez sur Enregistrer. Pour plus d'informations sur la stratégie de mot de passe, consultez la section « Gestion des mots de passe » à la page 47.

***Remarque :** si vous sélectionnez l'option Supprimer des utilisateurs et des groupes, durant la synchronisation, tous les utilisateurs externes qui ont été supprimés du serveur LDAP sont également supprimés du serveur Connect Pro.*

10. Consultez un aperçu de la synchronisation.

Ouvrez l'onglet Synchroniser les actions. Dans la section Aperçu de la synchronisation des annuaires, cliquez sur Aperçu. Pour plus d'informations, consultez la section « Recommandations relatives à la synchronisation » à la page 47.

Gestion des mots de passe

Si vous n'activez pas l'authentification LDAP, vous devez choisir comment Connect Pro authentifie les utilisateurs.

Lorsque Connect Pro importe les informations d'utilisateurs à partir d'un annuaire externe, il n'importe pas les mots de passe réseau. Vous devez donc implémenter une autre méthode de gestion des mots de passe pour les utilisateurs importés dans l'annuaire Connect Pro.

Notification des utilisateurs pour définir leur mot de passe

Dans l'écran Paramètres de la stratégie de l'onglet Paramètres de synchronisation, vous pouvez opter pour l'envoi d'un message électronique aux utilisateurs importés avec un lien qui leur permettra de définir leur mot de passe.

Définition du mot de passe sur un attribut LDAP

Vous pouvez choisir de définir le premier mot de passe d'un utilisateur importé sur la valeur d'un attribut d'entrée d'annuaire de cet utilisateur. Par exemple, si l'annuaire LDAP contient un champ de numéro ID d'employé, vous pouvez faire de cette valeur le mot de passe initial des utilisateurs. Lorsque les utilisateurs se connectent à l'aide de ce mot de passe, ils peuvent alors le modifier.

Recommandations relatives à la synchronisation

En tant qu'administrateur, deux méthodes vous permettent de synchroniser Connect Pro avec un annuaire LDAP externe :

- Vous pouvez planifier la synchronisation pour qu'elle ait lieu à intervalles réguliers.
- Vous pouvez effectuer une synchronisation manuelle qui synchronise immédiatement l'annuaire de Connect Pro et l'annuaire LDAP de l'organisation.

Avant d'importer les utilisateurs et les groupes dans une première synchronisation, il est préférable de vérifier les paramètres de connexion à l'aide d'un navigateur LDAP. Les navigateurs suivants sont disponibles en ligne : Navigateur/Editeur LDAP et Administrateur LDAP.

***Important :** pendant la synchronisation, ne relancez pas votre serveur LDAP et n'exécutez aucune tâche parallèle. En effet, cela entraînerait la suppression d'utilisateurs ou de groupes dans Connect Pro.*

Synchronisations planifiées

Les synchronisations planifiées sont recommandées, car elles garantissent que Connect Pro dispose d’une image à jour des utilisateurs et groupes importés depuis le répertoire LDAP de l’organisation.

Si vous importez un grand nombre d'utilisateurs et de groupes, il se peut que la synchronisation initiale exploite une grande quantité de ressources. Si c'est le cas, il est recommandé de planifier cette synchronisation initiale pendant une période creuse, la nuit par exemple. (Vous pouvez également effectuer la première synchronisation manuellement.)

Pour configurer une synchronisation planifiée, utilisez la fenêtre Paramètres de synchronisation > Paramètres de planification de la Console de gestion des applications.

Lorsqu'une synchronisation a lieu, Connect Pro compare les entrées de l'annuaire LDAP à celles de l'annuaire de Connect Pro et n'importe que celles dont au moins un champ a été modifié.

Aperçu de la synchronisation

Avant l'importation d'utilisateurs et de groupes dans la première synchronisation, Adobe vous recommande de tester vos mappages en affichant un aperçu de la synchronisation. Dans un aperçu, les utilisateurs et groupes ne sont pas à proprement parler importés, mais les erreurs sont enregistrées dans un journal. Vous pouvez alors examiner ces erreurs afin de diagnostiquer les problèmes éventuels.

Pour accéder aux journaux de synchronisation, utilisez la fenêtre Journaux de synchronisation. Chaque ligne du journal présente un événement de synchronisation et la synchronisation produit au moins un événement par utilisateur ou groupe traité. Si des avertissements ou des erreurs sont générés pendant l'aperçu, ils sont inscrits dans une liste dans un second journal d'avertissements.

Valeurs des fichiers journaux

Les journaux de synchronisation stockent les valeurs dans un format séparé par des virgules. Dans les tableaux suivants, le terme *principal* (mandant) fait référence aux entrées d'utilisateur et de groupe. Les valeurs suivantes sont incluses dans les entrées des journaux :

Champ	Description
Date	Valeur de date et d'heure, cette dernière allant jusqu'aux millisecondes. Le format est *aaaaMMjj'T'HHmmss.SSS*.
ID mandant	Nom de connexion ou nom du groupe.
Type de mandant	Caractère unique : U pour utilisateur, G pour groupe.
Evénement	L'action entreprise ou la condition rencontrée.
Détail	Informations détaillées sur l'événement.

Le tableau suivant présente les différents types d'événements pouvant apparaître dans les fichiers journaux de synchronisation.

Evénement	**Description**	**Détail**
add	Le mandant a été ajouté dans Connect Pro.	Paquet XML abrégé décrivant les champs mis à jour à l'aide d'une série de paires de balises au format ***<fieldname>valeur</fieldname>*** (par exemple, `<first-name>Joe</first-name>`). Le nœud parent et les champs non mis à jour sont omis.
update	Le mandant est un utilisateur externe et certains champs ont été mis à jour.	

update-members	Le mandant est un groupe externe et des mandants ont été ajoutés ou supprimés dans le groupe.	Paquet XML abrégé décrivant les membres supprimés et ajoutés. Le nœud parent est omis :
		`<add>ID list</add>`
		`<remove>ID list</remove>`
		La liste d'ID est une série de paquets `<id>principal ID</id>` où `principal ID` est un ID répertorié dans la colonne ID mandant, tel qu'un nom d'utilisateur ou un nom de groupe. S'il n'existe aucun membre d'une liste d'ID, le nœud parent est généré comme `<add/>` ou `<remove/>`.

delete	Le mandant a été supprimé de Connect pro.	
up-to-date	Le mandant est un mandant externe dans Connect Pro et est déjà synchronisé avec l'annuaire externe. Aucun changement n'a été effectué.	Un utilisateur ou un groupe créé dans Connect Pro est considéré comme un mandant interne. Un utilisateur ou un groupe créé par le processus de synchronisation est considéré comme un mandant externe.
make-external	Le mandant est un mandant interne de Connect Pro et a été converti en mandant externe.	Cet événement permet à la synchronisation de modifier ou de supprimer le mandant et est généralement suivi d'un autre événement qui fait l'un ou l'autre. Cet événement est consigné dans le journal d'avertissement.
warning	Un événement de niveau avertissement est survenu.	Message d'avertissement.
error	Une erreur s'est produite.	Message d'exception Java.

A propos du protocole LDAPS

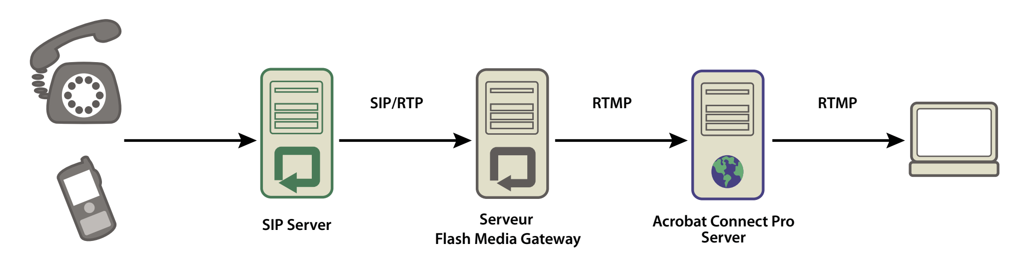
Connect Pro prend nativement en charge le protocole *LDAPS* (protocole LDAP sécurisé). Le serveur d'annuaire LDAP doit fournir une connexion SSL. Pour établir une connexion sécurisée à un serveur d'annuaire LDAP, utilisez le protocole LDAPS dans l'URL de connexion, comme dans l'exemple suivant : ldaps:// *ServeurAnnuaireExemple* : *NumeroPort*.

Déploiement de la fonctionnalité de voix universelle

Flux de travaux pour le déploiement de la fonctionnalité de voix universelle

Remarque : *pour obtenir une comparaison de la fonctionnalité de voix universelle et des adaptateurs de téléphonie intégrés, consultez la section* *« Options de conférence audio Connect Pro » à la page 16.*

La fonctionnalité de voix universelle utilise un composant appelé Flash Media Gateway pour recevoir du son d'un serveur SIP. Le son est transmis dans une direction, depuis un serveur SIP vers les salles de réunion Connect Pro. Installez Flash Media Gateway et configurez-le pour communiquer avec un serveur SIP. Le serveur SIP peut être hébergé par un tiers ou une partie de l'infrastructure de l'entreprise. (Les fournisseurs SIP sont également appelés *fournisseurs VoIP*.)



Le son est émis depuis un téléphone, passe par un serveur de conférence audio (non représenté), par un serveur SIP puis par Flash Media Gateway, pour arriver à une salle de réunion Connect Pro.

Suivez ce flux de travaux pour implémenter la solution de voix universelle :

1 Pour installer et configurer la fonctionnalité de voix universelle, vous devez être en possession des éléments suivants :

- Connect Pro 7.5 Service Pack 1 (SP1)
- Informations de connexion du fournisseur SIP

2 Installez Flash Media Gateway.

Vous pouvez installer Flash Media Gateway sur le même ordinateur que Connect Pro Server ou sur un ordinateur dédié. Vous pouvez déployer Flash Media Gateway sur un seul ordinateur ou sur un cluster de serveurs. Le programme d'installation de Flash Media Gateway fait partie du programme d'installation de Connect Pro Server. Consultez la section « Exécution du programme d'installation » à la page 27.

3 Configurez Flash Media Gateway pour vous connecter à un serveur SIP.

Une fois l'installation terminée, la Console de gestion des applications se lance. (Vous pouvez également accéder à la Console de gestion des applications à l'adresse http://localhost:8510/console.) Utilisez la console pour configurer Flash Media Gateway afin de vous connecter à un serveur SIP.

4 Ouvrez les ports. Consultez la section « Ports et protocoles Flash Media Gateway » à la page 50.

Si un pare-feu utilise un système NAT, reportez-vous à la section « Configuration de Flash Media Gateway afin d'établir la communication derrière un pare-feu utilisant un système NAT » à la page 51.

5 Pour installer Flash Media Gateway sur un cluster d'ordinateurs, consultez « Déploiement de Flash Media Gateway sur un cluster de serveurs » à la page 54.

6 Pour créer une séquence de connexion et tester la connexion audio, consultez la page www.adobe.com/go/learn_cnn_uvconfig_fr.

7 Si vous n'entendez pas le son dans une réunion Connect Pro, reportez-vous à la section « Résolution des problèmes liés à la fonctionnalité de voix universelle » à la page 55.

Ports et protocoles Flash Media Gateway

***Remarque :** pour afficher le schéma de flux de données entre un fournisseur SIP, Flash Media Gateway et Connect Pro Server, consultez la section « Flux de données » à la page 8.*

Flash Media Gateway écoute les requêtes du serveur d'application Connect Pro Central sur le port suivant :

Numéro de port	Adresse de liaison	Protocole
2222	*/Adaptateur quelconque	HTTP

Flash Media Gateway lance une connexion avec Flash Media Server comme un client RTMP régulier. Flash Media Server écoute Flash Media Gateway sur le port suivant :

Numéro de port	Adresse de liaison	Protocole
8506	*/Adaptateur quelconque	RTMP

Flash Media Gateway communique avec le fournisseur de conférences audio via les protocoles SIP et RTP sur les ports suivants :

Sens	Règle
Flash Media Gateway vers Internet	SRC-IP=<Server-IP>, SRC-PORT=5060, DST-IP=ANY, DST-PORT=5060
Internet vers Flash Media Gateway	SRC-IP=ANY, SRC-PORT=5060, DST-IP=<Server-IP>, DST-PORT=5060
Flash Media Gateway vers Internet	SRC-IP=<Server-IP>, SRC-PORT=5000_TO_6000, DST-IP=ANY, DST-PORT=ANY_HIGH_END
Internet vers Flash Media Gateway	SRC-IP=ANY, SRC-PORT=ANY_HIGH_END, DST-IP=<Server-IP>, DST-PORT=5000_TO_6000

Remarque : *ANY_HIGH_END implique tous les ports supérieurs à 1024. La gamme de ports par défaut s'étend de 5000 à 6000. Vous pouvez modifier ces valeurs dans la Console de gestion des applications.*

Configuration de Flash Media Gateway afin d'établir la communication derrière un pare-feu utilisant un système NAT

Remarque : *Vous n'avez pas besoin d'effectuer cette tâche si votre pare-feu est compatible SIP. De la même manière, dans certains cas, la passerelle de niveau application pour SIP dans un pare-feu peut provoquer des problèmes. Si vous ne parvenez pas à établir de communication par l'intermédiaire de la passerelle de niveau application, désactiver cette passerelle pour SIP dans le pare-feu et utilisez la technique décrite dans cette section.*

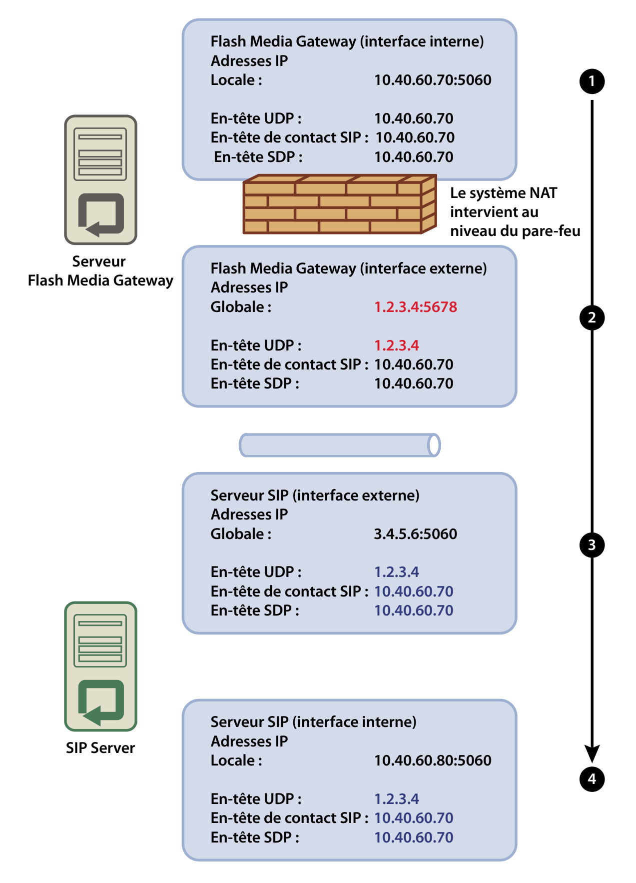
Le décodage d'adresses réseau (NAT) est un processus qui permet aux réseaux d'utiliser moins d'adresses IP externes et de masquer les adresses IP internes. NAT modifie l'adresse IP et le numéro de port des paquets émanant d'un réseau. Les adresses IP internes sont modifiées en adresse IP externe. NAT essaie également de diriger les réponses envoyées vers l'adresse IP externe vers les adresses IP internes correctes.

Si Flash Media Gateway se trouve derrière un pare-feu qui utilise NAT, il se peut qu'il ne puisse pas recevoir de paquets depuis le serveur SIP. NAT modifie l'adresse IP locale et l'adresse IP de l'en-tête UDP (source du paquet) pour qu'elle corresponde à l'adresse IP externe.

L'adresse IP de l'en-tête UDP est identique à l'adresse IP de Flash Media Gateway. Par conséquent, si le serveur SIP utilise l'adresse IP de l'en-tête UDP pour envoyer une réponse, la réponse trouve Flash Media Gateway.

L'adresse IP de l'en-tête de contact est identique à l'adresse IP de Flash Media Gateway. Par conséquent, si le serveur SIP utilise l'adresse IP de l'en-tête de contact pour envoyer une réponse, la réponse ne peut pas trouver Flash Media Gateway. L'adresse IP locale se cache derrière le pare-feu et n'est pas visible sur le serveur SIP.

L'image suivante montre comment NAT modifie les adresses IP sur le pare-feu :



NAT modifie l'adresse IP

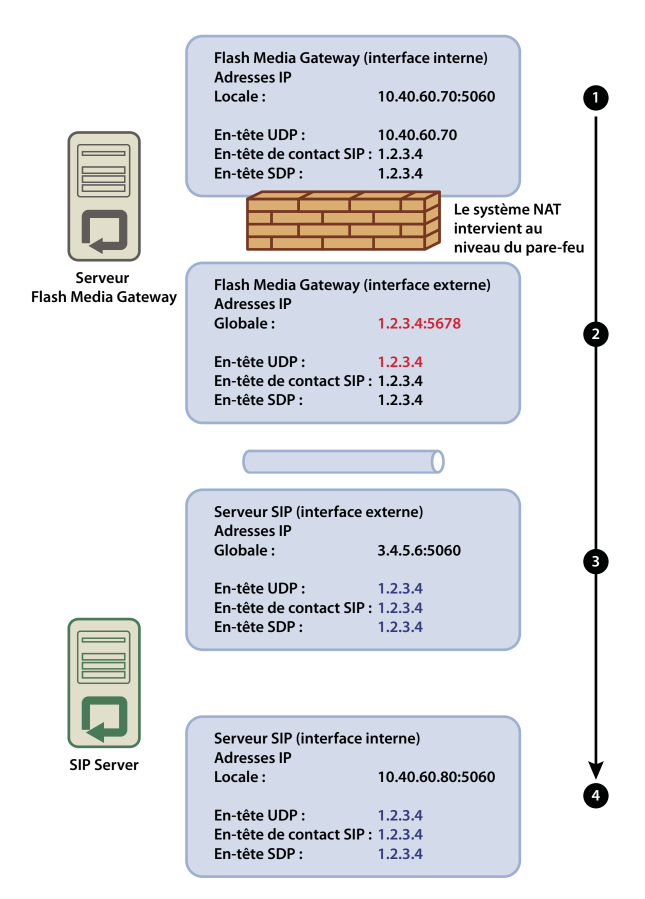
1 Flash Media Gateway (interface interne). L'en-tête UDP (adresse IP de la source du paquet) et l'adresse IP de l'en-tête de contact SIP sont identiques à l'adresse IP locale.

2 Flash Media Gateway (interface externe). NAT modifie l'adresse IP de l'en-tête UDP en adresse IP globale.

3 Serveur SIP (interface externe). Le paquet atteint l'interface globale sur le serveur SIP. Pour atteindre l'interface interne, transférez le port directement. Si le port n'est pas transféré, le paquet est perdu et la communication échoue.

4 Serveur SIP (interface interne). Le paquet est traité quand il atteint cette interface. Si le serveur SIP utilise l'adresse IP de l'en-tête UDP pour envoyer une réponse, la réponse atteint avec succès Flash Media Gateway. Si le serveur SIP utilise l'adresse IP de l'en-tête de contact, la réponse ne peut pas atteindre Flash Media Gateway.

L'image suivante montre une configuration réussie dans laquelle l'adresse IP de l'en-tête de contact SIP est identique à l'adresse IP externe de Flash Media Gateway. Cette modification permet de diriger les paquets vers Flash Media Gateway depuis le serveur SIP.



Configuration permettant une communication réussie

Pour vérifier que Flash Media Gateway peut bien recevoir des paquets depuis un serveur SIP, procédez comme suit :

1 Sur Flash Media Gateway, ouvrez le fichier *[rép_install_racine]*/conf/sip.xml dans un éditeur de texte. (Le dossier d'installation racine par défaut est C:\Program Files\Adobe\Flash Media Gateway.)

a Créez une balise `<globalAddress>` sous la balise `<Profile>`. Saisissez l'adresse IP externe de Flash Media Gateway, comme suit :

```
...
<Profiles>
    <Profile>
        <profil e I D>   s ipGateway </profileID>
        <userName>141583220 00 </ userName>
        <password></password>
        <displayName> sipGateway </displayName>
        <registrarAddress>8.15.247.100:5060</registrarAddress>
        <doRegister>0</doRegister>
        <defaulthost>8.15.247.100:5060</defaulthost>
        <hostPort> 0 </hostPort>
        <context> sipGatewayContext </context>
        <globalAddress>8.15.247.49</globalAddress>
        <supportedCodecs><codecID> G711u </codecID><codecID> speex </codecID>
    </supportedCodecs>
    </Profile>
</Profiles>
...
```

Dans un cluster, chaque serveur Flash Media Gateway doit avoir une adresse IP externe unique.

***Important :** si l'adresse IP externe est dynamique, vous devrez reconfigurer Flash Media Gateway à chaque fois que l'adresse IP externe change.*

b Redémarrez le service Flash Media Gateway. Voir « Démarrage et arrêt de Flash Media Gateway » à la page 105.

2 Sur le pare-feu situé entre le serveur Flash Media Gateway et le serveur SIP, transférez directement le port SIP (5060 par défaut) et tous les ports voix RTP (5000 - 6000 par défaut) vers le serveur Flash Media Gateway. Les ports ouverts sur le pare-feu doivent être identiques à ceux ouverts sur le serveur Flash Media Gateway.

***Remarque :** Les serveurs peuvent communiquer sans transfert des ports. Toutefois, sans transfert des ports, les appels risquent de se déconnecter inopinément, notamment après des durées prolongées.*

Configuration du niveau de connexion de Flash Media Gateway

Un niveau élevé de connexion peut provoquer des bruits parasites lorsque la charge sur Flash Media Gateway est élevée. Les niveaux élevés de connexion inscrivent plus d'informations dans le journal. L'inscription dans le journal requiert une grande puissance de traitement au détriment de la transmission du son. Pour des performances optimales, Adobe recommande de définir le niveau de connexion des données audio sur 4.

1 Ouvrez le fichier fmsmg.xml dans un éditeur de texte (par défaut, le fichier se trouve dans le répertoire C:\Program Files\Adobe\Flash Media Gateway\conf.).

2 Définissez la valeur `logLevel` sur 4 :

```
<logLevel>4</logLevel>
```

3 Redémarrez Flash Media Gateway.

Déploiement de Flash Media Gateway sur un cluster de serveurs

L'application Flash Media Gateway installée sur un ordinateur avec deux processeurs peut passer 100 appels simultanément. Pour gérer une charge plus élevée, augmentez le nombre de processeurs ou ajoutez des serveurs Flash Media Gateway supplémentaires dans le cluster.

Pour déployer un cluster de serveurs, installez Flash Media Gateway sur ses propres ordinateurs et Connect Pro Server sur ses ordinateurs également. N'installez pas Connect Pro Server et Flash Media Gateway sur les mêmes ordinateurs.

Lorsque vous déployez Flash Media Gateway sur un cluster de serveurs, Connect Pro Server traite l'équilibrage des charges et la reprise. La connexion à Pro Edge Server ne nécessite pas de configuration supplémentaire.

1 Exécutez le programme d'installation sur chaque serveur du cluster et choisissez d'installer Flash Media Gateway. Consultez la section « Exécution du programme d'installation » à la page 27.

   Remarque : *pour plus d'informations sur le déploiement de Connect Pro Server dans un cluster, consultez la section « Déployer un cluster de serveurs Connect Pro » à la page 35.*

2 Sur un serveur Connect Pro, ouvrez la console de gestion des applications à l'adresse http://localhost:8510/console.

3 Sélectionnez Paramètres Flash Media Gateway et cliquez sur Ajouter pour ajouter et configurer des serveurs Flash Media Gateway supplémentaires.

   Remarque : *utilisez la Console de gestion des applications sur un serveur pour saisir les paramètres de configuration de tous les serveurs du cluster. La Console de gestion des applications envoie les paramètres de configuration à chaque serveur du cluster.*

Résolution des problèmes liés à la fonctionnalité de voix universelle

Si vous n'entendez pas le son d'une conférence audio Universal Voice dans une salle de réunion, effectuez les opérations suivantes :

1 Vérifiez que le volume est activé sur l'ordinateur. Si vous utilisez des écouteurs, vérifiez qu'ils sont branchés correctement dans la prise de sortie audio.

2 Testez la séquence de numérotation. Reportez-vous à Test d'une séquence de numérotation.

3 Assurez-vous que Flash Media Gateway est correctement configuré :

   a Ouvrez la Console de gestion des applications (http://localhost:8510/console) sur Connect Pro Server et cliquez sur Paramètres de Flash Media Gateway. Chaque instance Flash Media Gateway doit avoir l'état Actif.

   b Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server > Configurer Connect Pro Server.

   c Si l'état n'est pas Actif, ouvrez le fichier *[rép_install_racine]*/custom.ini. Vérifiez que les entrées suivantes y figurent :

```
FMG_ADMIN_USER=sa
FMG_ADMIN_PASSWORD=breeze
```

   Si vous ne voyez pas ces entrées, saisissez-les et redémarrez le serveur d'application de Connect Pro Central.

4 Contactez l'Assistance technique d'Adobe à l'adresse www.adobe.com/go/connect_licensed_programs_fr.

Déploiement d'adaptateurs de téléphonie intégrés

Les adaptateurs de téléphonie intégrés sont des extensions Java qui permettent à Connect Pro de se connecter à un pont audio. Vous pouvez installer le nombre d'adaptateurs de téléphonie intégrés de votre choix lorsque vous installez Connect Pro. Pour plus d'informations, voir « Préparation de l'installation des adaptateurs de téléphonie intégrés » à la page 17.

Après l'installation d'un ou de plusieurs adaptateurs, voir les sections suivantes pour vérifier et configurer l'installation.

- « Adaptateur de téléphonie Avaya » à la page 56
- « Adaptateur de téléphonie InterCall » à la page 56

- « Adaptateur de téléphonie MeetingOne » à la page 57
- « Adaptateur de téléphonie PGi (NA) » à la page 58
- « Adaptateur de téléphonie PGi (EMEA) » à la page 58

Si vous souhaitez configurer d'autres fonctionnalités d'adaptateur après l'installation, voir la TechNote à l'adresse www.adobe.com/go/learn_cnn_customize_adaptor_fr.

Adaptateur de téléphonie Avaya

Effectuez les deux tâches suivantes pour vérifier que l'adaptateur fonctionne comme prévu.

Vérification de l'activation du système de téléphonie

1 Connectez-vous à Connect Pro Central.

2 Cliquez sur Administration > Fournisseurs audio.

  Si le système de téléphonie est activé correctement, Meeting Exchange figure dans la liste des fournisseurs. Sélectionnez Meeting Exchange et cliquez sur Modifier afin d'activer ou de désactiver l'adaptateur pour l'intégralité du compte Connect Pro.

3 Pour ajouter un profil audio Meeting Exchange, cliquez sur Mon profil > Mes profils audio > Nouveau profil. Dans la liste des fournisseurs, sélectionnez Meeting Exchange.

  Pour plus d'informations, voir Utilisation d'Acrobat Connect Pro.

Test du son dans une réunion

❖ Avant de déployer Connect Pro dans un environnement de production, enregistrez au moins 2 minutes d'une réunion. Consultez l'archive de la réunion pour vérifier que le son a été enregistré correctement.

Désactivation de l'adaptateur

Si vous souhaitez désactiver l'adaptateur Avaya :

1 Arrêtez·Connect Pro.

2 Ouvrez le fichier *[rép_install_racine]*\telephony-service\conf\telephony-settings.xml.

3 Définissez l'attribut `enabled` de la balise `<telephony-adaptor>` sur `false`, comme dans l'exemple suivant :

```
<telephony-adaptor id="avaya-adaptor" class-
name="com.macromedia.breeze_ext.telephony.AvayaAdaptor" enabled="false">
```

4 Redémarrez Connect Pro.

Adaptateur de téléphonie InterCall

Effectuez les deux tâches suivantes pour vérifier que l'adaptateur fonctionne comme prévu.

Vérification de l'activation du système de téléphonie

1 Connectez-vous à Connect Pro Central.

2 Cliquez sur Administration > Fournisseurs audio.

  Si le système de téléphonie est activé correctement, InterCall figure dans la liste des fournisseurs. Sélectionnez InterCall et cliquez sur Modifier afin d'activer ou de désactiver l'adaptateur pour l'intégralité du compte Connect Pro.

3 Pour ajouter un profil audio InterCall, cliquez sur Mon profil > Mes profils audio > Nouveau profil. Dans la liste des fournisseurs, sélectionnez InterCall.

Pour plus d'informations, voir Utilisation d'Acrobat Connect Pro.

Test du son dans une réunion

Avant de déployer Connect Pro dans un environnement de production, enregistrez au moins 2 minutes d'une réunion. Consultez l'archive de la réunion pour vérifier que le son a été enregistré correctement.

Désactivation de l’adaptateur de téléphonie

Si vous souhaitez désactiver l’adaptateur InterCall :

1 Arrêtez·Connect Pro.

2 Ouvrez le fichier *[rép_install_racine]*\TelephonyService\conf\telephony-settings.xml.

3 Définissez l'attribut `enabled` de la balise `<telephony-adaptor>` sur `false`, comme dans l'exemple suivant :

```
<telephony-adaptor id="intercall-adaptor" class-
name="com.macromedia.breeze_ext.telephony.Intercall.IntercallTelephonyAdaptor"
enabled="false">
```

4 Redémarrez Connect Pro.

Adaptateur de téléphonie MeetingOne

Effectuez les deux tâches suivantes pour vérifier que l'adaptateur fonctionne comme prévu.

Vérification de l'activation du système de téléphonie

1 Connectez-vous à Connect Pro Central.

2 Cliquez sur Administration > Fournisseurs audio.

Si le système de téléphonie est activé correctement, MeetingOne figure dans la liste des fournisseurs. Sélectionnez MeetingOne et cliquez sur Modifier afin d’activer ou de désactiver l’adaptateur pour l’intégralité du compte Connect Pro.

3 Pour ajouter un profil audio MeetingOne, cliquez sur Mon profil > Mes profils audio > Nouveau profil. Dans la liste des fournisseurs, sélectionnez MeetingOne.

Pour plus d'informations, voir Utilisation d'Acrobat Connect Pro.

Test du son dans une réunion

Avant de déployer Connect Pro dans un environnement de production, enregistrez au moins 2 minutes d'une réunion. Consultez l'archive de la réunion pour vérifier que le son a été enregistré correctement.

Désactivation de l'adaptateur de téléphonie

Si vous souhaitez désactiver l’adaptateur MeetingOne :

1 Arrêtez·Connect Pro.

2 Ouvrez le fichier *[rép_install_racine]*\TelephonyService\conf\telephony-settings.xml.

3 Définissez l'attribut `enabled` de la balise `<telephony-adaptor>` sur `false`, comme dans l'exemple suivant :

```
<telephony-adaptor id="meetingone-adaptor" class-
name="com.meetingone.adobeconnect.MeetingOneAdobeConnectAdaptor" enabled="false">
```

4 Redémarrez Connect Pro.

Adaptateur de téléphonie PGi (NA)

Effectuez les trois tâches suivantes pour vérifier que l'adaptateur fonctionne comme prévu.

Configuration des noms de domaine

Connect Pro utilise le protocole HTTP sur le port 443 pour communiquer avec l'adaptateur PGi. Vérifiez que Connect Pro peut communiquer avec le domaine **csaxis.premconf.com**.

Vérification de l'activation du système de téléphonie

1 Connectez-vous à Connect Pro Central.

2 Cliquez sur Administration > Fournisseurs audio.

Si le système de téléphonie est activé correctement, Premiere NA figure dans la liste des fournisseurs. Sélectionnez Premiere NA et cliquez sur Modifier afin d'activer ou de désactiver l'adaptateur pour l'intégralité du compte Connect Pro.

3 Pour ajouter un profil audio Premiere NA, cliquez sur Mon profil > Mes profils audio > Nouveau profil. Dans la liste des fournisseurs, sélectionnez Premiere NA.

Pour plus d'informations, voir Utilisation d'Acrobat Connect Pro.

Test du son dans une réunion

Avant de déployer Connect Pro dans un environnement de production, enregistrez au moins 2 minutes d'une réunion. Consultez l'archive de la réunion pour vérifier que le son a été enregistré correctement.

Désactivation de l'adaptateur de téléphonie

Si vous souhaitez désactiver l'adaptateur Premiere NA :

1 Ouvrez le fichier *[rép_install_racine]*\TelephonyService\conf\telephony-settings.xml.

2 Définissez l'attribut `enabled` de la balise `<telephony-adaptor>` sur `false`, comme dans l'exemple suivant :

```
<telephony-adaptor id="premiere-adaptor" class-
name="com.macromedia.breeze_ext.premiere.gateway.PTekGateway" enabled="false">
```

3 Redémarrez Connect Pro.

Adaptateur de téléphonie PGi (EMEA)

Effectuez les trois tâches suivantes pour vérifier que l'adaptateur fonctionne comme prévu.

Configuration des noms de domaine

Connect Pro utilise le protocole HTTP sur le port 443 pour communiquer avec l'adaptateur PGi. Vérifiez que Connect Pro peut communiquer avec le domaine **euaxis.premconf.com**.

Vérification de l'activation du système de téléphonie

1 Connectez-vous à Connect Pro Central.

2 Cliquez sur Administration > Fournisseurs audio.

Si le système de téléphonie est activé correctement, l'adaptateur PGi EMEA figure dans la liste des fournisseurs. Sélectionnez PGi pour la région EMEA et cliquez sur Modifier afin d'activer ou de désactiver l'adaptateur pour l'intégralité du compte Connect Pro.

3 Pour ajouter un profil audio PGi pour la région EMEA, cliquez sur Mon profil > Mes profils audio > Nouveau profil. Dans la liste des fournisseurs, sélectionnez PGi pour la région EMEA.

Pour plus d'informations, voir Utilisation d'Acrobat Connect Pro.

Test du son dans une réunion

Avant de déployer Connect Pro dans un environnement de production, enregistrez au moins 2 minutes d'une réunion. Consultez l'archive de la réunion pour vérifier que le son a été enregistré correctement.

Désactivation de l'adaptateur de téléphonie

Si vous souhaitez désactiver l'adaptateur PGi EMEA :

1 Ouvrez le fichier *[rép_install_racine]*\TelephonyService\conf\telephony-settings.xml.

2 Définissez l'attribut `enabled` de la balise `<telephony-adaptor>` sur `false`, comme dans l'exemple suivant :

```
<telephony-adaptor id="premiere-emea-adaptor" class-
name="com.macromedia.breeze_ext.premiere.gateway.EMEA.PTekGateway" enabled="false">
```

3 Redémarrez Connect Pro.

Configuration du stockage partagé

A propos du stockage partagé

Vous pouvez utiliser le programme d'installation ou la Console de gestion des applications pour configurer Connect Pro afin qu'il gère le stockage de contenu avec des périphériques NAS et SAN. Le terme « contenu » désigne tout fichier publié dans Connect Pro, tel que des cours, des fichiers SWF, PPT ou PDF et des enregistrements archivés.

Configurations de stockage partagé possibles :

- Le contenu est copié sur les principaux périphériques de stockage externes et extrait vers le dossier de contenu de chaque serveur Connect Pro lorsque cela s'avère nécessaire. L'ancien contenu est purgé du dossier de contenu de chaque serveur afin de libérer de la place pour le nouveau contenu lorsque cela s'avère nécessaire. Cette configuration libère des ressources sur le serveur d'applications, ce qui se révèle particulièrement utile dans le cas d'un cluster volumineux. (Entrez une valeur dans les champs Stockage partagé et Taille du contenu mis en cache.)
- Le contenu est copié sur tous les serveurs et sur le principal périphérique de stockage externe. Cette configuration est recommandée pour les petits clusters, sauf si vous disposez d'une grande quantité de contenu dont l'accès est aléatoire. (Entrez une valeur dans le champ Stockage partagé ; ne renseignez pas le champ Taille du contenu mis en cache.)

Remarque : *si vous utilisez un cluster Connect Pro et que vous ne configurez pas les périphériques de stockage partagé, le cluster fonctionne en mode miroir complet (le contenu publié dans Connect Pro est copié sur tous les serveurs) et le contenu n'est jamais supprimé automatiquement d'aucun serveur.*

Configuration du stockage partagé

Si vous n’avez pas configuré de stockage partagé pendant l’installation, vous pouvez le faire en suivant les instructions de cette section.

- Si vous configurez un stockage partagé pour un seul serveur Connect Pro, suivez les instructions de la première tâche.
- Si vous configurez un stockage partagé pour un cluster, suivez les instructions de la première tâche pour un ordinateur du cluster, puis les instructions de la seconde tâche pour tous ses autres ordinateurs.

Voir aussi

« Périphériques de stockage de contenu pris en charge » à la page 5

« Déployer un cluster de serveurs Connect Pro » à la page 35

C*onfiguration du stockage partagé

Avant de commencer, Connect Pro doit être configuré sans stockage partagé et s'exécuter sur un serveur.

1 Configurez un volume partagé sur un périphérique de stockage externe.

Si le volume partagé présente un nom d'utilisateur et un mot de passe, tous les volumes partagés doivent utiliser le même nom d'utilisateur et le même mot de passe.

2 (Facultatif) Si vous actualisez un serveur Connect Pro existant afin d'utiliser des volumes de stockage partagés, vous devez copier le contenu de l'un de ces serveurs sur le volume partagé.

a Arrêtez le serveur (Démarrer > Programmes > Adobe Acrobat Connect Pro Server > Arrêter Connect Pro Central Application Server et Arrêter Connect Pro Meeting Server).

b Copiez le dossier *[rép_install_racine]*\content\7 dans le volume partagé créé à l'étape 1.

Il se peut que certains ordinateurs d'un cluster présentent du contenu supplémentaire. Connect Pro ne peut pas utiliser ces fichiers, mais si vous souhaitez les copier sur le volume partagé pour les archiver, vous pouvez rédiger et exécuter un script qui compare le contenu de chaque ordinateur avec celui du volume partagé.

c Démarrez Connect Pro (Démarrer > Programmes > Adobe Acrobat Connect Pro Server > Démarrer Connect Pro Meeting Server et Démarrer Connect Pro Central Application Server).

3 Dans Connect Pro Server, choisissez Démarrer > Panneau de configuration > Outils d’administration > Services pour ouvrir la fenêtre Services, sélectionnez Adobe Acrobat Connect Pro Service, puis procédez comme suit :

a Cliquez avec le bouton droit et sélectionnez Propriétés.

b Sélectionnez l'onglet Connexion.

c Sélectionnez Ce compte et, si le volume partagé possède un nom d'utilisateur et un mot de passe, entrez-les, puis cliquez sur Appliquer.

4 Redémarrez Connect Pro (serveur d'applications uniquement).

a Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server > Arrêter Connect Pro Central Application Server.

b Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server > Démarrer Connect Pro Central Application Server.

5 Ouvrez la Console de gestion des applications (Démarrer > Programmes > Adobe Acrobat Connect Pro Server > Configurer Connect Pro Server).

6 Dans l'onglet Paramètres de l'application, ouvrez l'onglet Paramètres du serveur, localisez la section Paramètres du stockage partagé et entrez un chemin de dossier dans le champ Stockage partagé (par exemple, **\\stockage**).

Si le périphérique de stockage principal est plein, vous pouvez ajouter un autre périphérique à l'emplacement principal. Séparez les chemins par des points-virgules (;) : **\\nouveau-stockage;\\stockage**.

Remarque : *l'écriture (copie dans le dossier de stockage) s'effectue uniquement dans le premier dossier. La lecture (copie depuis le dossier de stockage) s'effectue en séquence, en commençant par le premier dossier jusqu'à ce que le fichier soit localisé.*

7 (Facultatif) Pour configurer le dossier de contenu sur Connect Pro pour faire office de cache (des ressources sont supprimées automatiquement lorsque de l'espace est nécessaire et rétablies sur demande), entrez une valeur dans la zone Taille du contenu mis en cache.

La taille du cache du contenu correspond à un pourcentage de l'espace disque devant être utilisé comme cache. Adobe recommande de définir une valeur comprise entre 15 et 50, car le cache peut grossir bien au-delà de la taille définie. Le cache n'est purgé que lorsque le contenu affiché a expiré (24 heures après sa dernière consultation).

8 Cliquez sur Enregistrer et fermez la Console de gestion des applications.

9 Redémarrez Connect Pro (serveur d'applications uniquement).

a Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server > Arrêter Connect Pro Central Application Server.

b Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server > Démarrer Connect Pro Central Application Server.

Configuration du stockage partagé pour d'autres serveurs d'un cluster

1 Installez Connect Pro sans le démarrer. Si Connect Pro est installé et déjà en cours d'exécution, arrêtez-le.

2 Dans Connect Pro Server, choisissez Démarrer > Panneau de configuration > Outils d'administration > Services pour ouvrir la fenêtre Services, sélectionnez Adobe Acrobat Connect Pro Service, puis procédez comme suit :

a Cliquez avec le bouton droit et sélectionnez Propriétés.

b Sélectionnez l'onglet Connexion.

c Sélectionnez Ce compte et, si le volume partagé possède un nom d'utilisateur et un mot de passe, entrez-les, puis cliquez sur Appliquer.

3 Démarrez Connect Pro.

a Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server > Démarrer Connect Pro Meeting Server.

b Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server > Démarrer Connect Pro Central Application Server.

4 (Facultatif) Si vous installez Connect Pro pour la première fois, suivez les étapes indiquées à la section « Déployer un cluster de serveurs Connect Pro » à la page 35.

5 Cliquez sur Enregistrer et fermez la Console de gestion des applications.

Configuration des liens à l'Aide et aux ressources

Ajout de liens Prise en charge et Etat au menu d'aide

Les administrateurs de compte peuvent ajouter un lien de page Etat et un lien de page Support au menu d'aide dans les salles de réunion. Les liens mènent vers des pages HTML que vous concevez. La page Etat peut fournir des informations sur l'état actuel du système Connect Pro. La page Support peut fournir des informations sur l'obtention d'assistance concernant l'utilisation de Connect Pro. Si vous ne définissez pas ces liens, ils ne sont pas disponibles dans le menu Aide.

1 Ouvrez le fichier *RootInstallationFolder*\custom.ini dans un éditeur de texte.

2 Pour modifier le lien de page Etat, configurez `STATUS_PAGE = "http://connect.mycompany.com/status.html"`.

3 Pour modifier le lien de page Support, configurez `SUPPORT_PAGE="http://connect.mycompany.com/support.html"`.

Les URL peuvent être absolues ou relatives au domaine du serveur de réunions. Commencez les URL absolues par « http:// » ou « https:// ». Commencez les URL relatives par « / ».

4 Procédez comme suit pour redémarrer Connect Pro :

a Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server > Arrêter Connect Pro Central Application Server.

b Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server > Démarrer Connect Pro Central Application Server.

Redirection des liens vers les ressources de Connect Pro Central

La page d'accueil de Connect Pro Central dispose d'un onglet Ressources qui fournit des liens vers une page Mise en route, l'Aide de Connect Pro Central, la documentation Connect Pro et le Centre de ressources de Connect Pro. Vous pouvez rediriger ces liens vers d'autres emplacements.

1 Ouvrez la page que vous souhaitez modifier dans un éditeur HTML. Dans chaque chemin d'accès au fichier, remplacez l'espace réservé *lang* par le code de langue en deux lettres. Par exemple, le code de l'anglais est « en ».

Page	Emplacement	Notes
Prise en main	appserv/web/common/help/*lang*/support/startmain .htm	Vous pouvez modifier ce fichier dans Connect Pro Server version 7 et les versions ultérieures.
Aide de Connect Pro Central	appserv/web/common/help/lang/connect/AH_HOM E.html	La modification de ce fichier modifie également le lien vers l'Aide figurant en haut de la fenêtre Connect Pro Central. Vous pouvez modifier ce fichier dans Connect Pro Server version 7 et les versions ultérieures.
Centre de ressources Connect Pro	appserv/web/common/help/lang/go/resourceCente r.html	Vous pouvez modifier ce fichier dans Connect Pro Server version 7.5 et les versions ultérieures.
Documentation Connect Pro	appserv/web/common/help/lang/go/doc.html	Vous pouvez modifier ce fichier dans Connect Pro Server version 7.5 et les versions ultérieures.

2 Pour chacun de ces fichiers, insérez les informations suivantes en tant que contenu total du fichier :

```
<!-- =======================================================================
    This is used by Connect Pro to redirect to the desired webpage.
    If there is a particular place where you would like users to be sent,
    please customize the URL below.
     ======================================================================= -->
<META HTTP-EQUIV=Refresh CONTENT="0; URL=http://desiredpage.com">
```

3 Modifiez la valeur de l'attribut URL afin qu'il pointe vers votre contenu. L'URL peut être un chemin relatif ou absolu.

Par exemple, pour rediriger le fichier doc.html vers la documentation située sur le serveur de votre organisation, vous pouvez utiliser l'URL http://www.masociété.com/support/documentation/connectpro.

Configuration des paramètres de notification de compte

Définition de l'heure d'envoi des rapports mensuels

Connect Pro vous envoie chaque mois un courrier électronique concernant la capacité de votre compte. Par défaut, les rapports mensuels de capacité de compte sont envoyés à 15h00 UTC. Pour que Connect Pro envoie le courrier électronique à une autre heure, vous pouvez ajouter des paramètres au fichier custom.ini et définir les valeurs souhaitées.

Pour plus d'informations sur la configuration des notifications de compte dans Connect Pro Central, reportez-vous au chapitre « Administration d'Acrobat Connect Pro » du document *Utilisation d'Adobe Acrobat Connect Pro* 7.5 disponible en ligne à l'adresse www.adobe.com/go/connect_documentation_fr.

1 Ouvrez le fichier *Rép_Install_Racine*\custom.ini et ajoutez les paramètres suivants au fichier avec les valeurs souhaitées :

THRESHOLD_MAIL_TIME_OF_DAY_HOURS Heure UTC à laquelle sont envoyés les rapports mensuels de notification de capacité. Cette valeur doit être un entier compris entre 0 et 23. Ce paramètre doit être défini dans le fichier custom.ini ; il ne peut pas être défini dans Connect Pro Central.

THRESHOLD_MAIL_TIME_OF_DAY_MINUTES Minute à laquelle sont envoyés les rapports mensuels de notification de capacité. Cette valeur doit être un entier compris entre 0 et 59. Ce paramètre doit être défini dans le fichier custom.ini ; il ne peut pas être défini dans Connect Pro Central.

***Remarque :** si l'un des paramètres précédents n'est pas spécifié ou est erroné, le courrier électronique est envoyé à 15h00 (UTC).*

Exemples de valeurs ajoutées au fichier custom.ini :

```
THRESHOLD_MAIL_TIME_OF_DAY = 5
THRESHOLD_MAIL_TIME_OF_MINUTES = 30
```

2 Procédez comme suit pour redémarrer Connect Pro :

a Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server > Arrêter Connect Pro Central Application Server.

b Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server > Démarrer Connect Pro Central Application Server.

Définition de seuils de capacité

Les administrateurs de compte Connect Pro peuvent définir des seuils de capacité dans Connect Pro Central. Le dépassement de ces seuils par un compte déclenche l'envoi d'une notification. Vous pouvez ajouter au fichier custom.ini des paramètres qui définissent les seuils de capacité par défaut dans Connect Pro Central.

Pour plus d'informations sur la configuration des notifications de compte dans Connect Pro Central, reportez-vous au chapitre « Administration d'Acrobat Connect Pro » du document *Utilisation d'Adobe Acrobat Connect Pro* 7.5 disponible en ligne à l'adresse www.adobe.com/go/connect_documentation_fr.

1 Ouvrez le fichier *Rép_Install_Racine*\custom.ini et ajoutez l'un des paramètres suivants au fichier avec les valeurs souhaitées :

THRESHOLD_NUM_OF_MEMBERS Pourcentage de seuil par défaut du quota d'auteurs et d'hôtes de réunion. Cette valeur doit être un entier compris entre 10 et 100 et divisible par 10. Si aucune valeur n'est spécifiée ou qu'elle est erronée, c'est la valeur 80 qui est utilisée.

THRESHOLD_CONC_USERS_PER_MEETING Pourcentage de seuil par défaut du quota d'utilisateurs simultanés par réunion. Cette valeur doit être un entier compris entre 10 et 100 et divisible par 10. Si aucune valeur n'est spécifiée ou qu'elle est erronée, c'est la valeur 80 qui est utilisée.

THRESHOLD_CONC_MEETING_USERS_PER_ACCOUNT Pourcentage de seuil par défaut du quota de participants à la réunion à l'échelle du compte. Cette valeur doit être un entier compris entre 10 et 100 et divisible par 10. Si aucune valeur n'est spécifiée ou qu'elle est erronée, c'est la valeur 80 qui est utilisée.

THRESHOLD_CONC_TRAINING_USERS Pourcentage de seuil par défaut du quota de stagiaires simultanés. Cette valeur doit être un entier compris entre 10 et 100 et divisible par 10. Si aucune valeur n'est spécifiée ou qu'elle est erronée, c'est la valeur 80 qui est utilisée.

Exemples de valeurs ajoutées au fichier custom.ini :

```
THRESHOLD_NUM_OF_MEMBERS = 90
THRESHOLD_CONC_USERS_PER_MEETING = 90
THRESHOLD_CONC_MEETING_USERS_PER_ACCOUNT = 90
THRESHOLD_CONC_TRAINING_USERS = 75
```

2 Procédez comme suit pour redémarrer Connect Pro :

a Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server > Arrêter Connect Pro Central Application Server.

b Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server > Démarrer Connect Pro Central Application Server.

Conversion PDF-SWF

A propos de la conversion de PDF

Vous pouvez utiliser le pod Share dans une salle de réunion Connect Pro pour partager des documents PDF. Les hôtes et les présentateurs peuvent synchroniser la navigation de tous les participants et utiliser le tableau blanc pour collaborer. Vous pouvez charger les documents PDF dans le pod Share depuis le bureau ou depuis la bibliothèque de contenu Connect Pro. Le partage de documents dans le pod Share offre les avantages suivants par rapport au partage d'écran :

- Les hôtes et les présentateurs peuvent précharger et organiser des documents dans la salle de réunion.
- Un affichage de meilleure qualité pour tous les participants.

- Exigence de bande passante inférieure pour les participants et les présentateurs.
- Collaboration facilitée pour les présentateurs multiples.
- Collaboration facilitée avec le tableau blanc.

Quand les documents PDF sont partagés dans un pod Share, Connect Pro les convertit au format Flash. Connect Pro Server propose des paramètres de configuration pour contrôler la conversion des PDF.

Configuration de la conversion PDF-SWF

1 Ouvrez le fichier *RootInstallationFolder*\custom.ini dans un éditeur de texte.

2 Modifiez l'un des paramètres de configuration suivants :

Paramètre	Valeur par défaut	Description
`ENABLE_PDF2SWF`	true	Valeur booléenne spécifiant si la conversion PDF-SWF est activée ou non pour le serveur. Définissez ce paramètre sur false pour désactiver la conversion en raison de problèmes de performance.
`PDF2SWF_PAGE_TIMEOUT`	5	La valeur du délai d'attente par page, en secondes.
`PDF2SWF_CONVERTER_PORTS_START`	4000	La plus petite valeur de la gamme de ports utilisés pour les conversions des PDF en SWF.
`PDF2SWF_CONVERTER_PORTS_END`	4030	La plus grande valeur de la gamme de ports utilisés pour les conversions des PDF en SWF.
`PDF2SWF_CONCURRENCY_LIMIT`	3	Le nombre maximal de conversions simultanées de PDF en SWF pouvant avoir lieur sur un serveur d'application. Si un serveur d'application reçoit plus de requêtes, les requêtes sont placées dans la file d'attente.
`PDF2SWF_QUEUE_LIMIT`	5	Le nombre maximal de conversions de PDF en SWF pouvant attendre dans une file d'attente en même temps. Si un serveur d'application reçoit plus de requêtes, un utilisateur voit le message suivant apparaître : « Connect Pro n'a pas pu convertir le fichier à afficher, veuillez réessayer ultérieurement. » Un administrateur voit s'afficher dans les journaux : <status code="request-retry"><exception>java.lang.Exception: Conversion Load too much on server.
`PDF2SWF_TIMEOUT_NUMBER_OF_PAGES`	3	Le nombre maximal de pages autorisées dans le délai d'attente avant l'arrêt de la conversion.

3 Redémarrez Connect Pro Central Application Server. Reportez-vous à la section « Démarrage et arrêt de Connect Pro » à la page 103.

Intégration à Microsoft Live Communications Server 2005 et Microsoft Office Communications Server 2007

Procédure de configuration de l'intégration de présence

Intégrez Connect Pro à un serveur de communications en temps réel Microsoft de manière à ce que les hôtes de réunion puissent voir la présence LCS ou OCS des participants à la réunion enregistrés dans la liste des invités et initier des conversations texte avec des utilisateurs en ligne.

Pour plus d'informations sur la liste des invités, reportez-vous au document *Utilisation d'Adobe Acrobat Connect Pro 7.5* disponible en ligne à l'adresse www.adobe.com/go/connect_documentation_fr.

1. Connect Pro Server et un serveur de communications doivent être installés.

Installez et vérifiez l'installation de Connect Pro Server et d'un serveur de communications. Connect Pro Server prend en charge l'intégration à Microsoft Live Communications Server 2005 et Microsoft Office Communications Server 2007. Reportez-vous à la section « Installation de Connect Pro 7.5 SP1 » à la page 27 et à la documentation du serveur de communications.

2. Configurez le serveur de communication.

Configurez le serveur de communication pour échanger des données avec Connect Pro. Voir « Configuration de Live Communications Server 2005 » à la page 66 ou « Configuration d'Office Communications Server 2007 » à la page 67.

3. Arrêtez Connect Pro Presence Service.

Connect Pro Presence Service fait partie de Connect Pro Server Arrêtez le service avant de configurer Connect Pro. Reportez-vous à la section « Démarrage et arrêt de Connect Pro Presence Service » à la page 72.

4. Configurez Connect Pro Presence Service.

Configurez Connect Pro pour échanger des données avec le serveur de communications. Le serveur de présence est installé sur *RootInstallationFolder*\presserv. Reportez-vous à la section « Configuration de Connect Pro Presence Service » à la page 69.

5. Démarrez Connect Pro Presence Service.

Reportez-vous à la section « Démarrage et arrêt de Connect Pro Presence Service » à la page 72.

6. Activez la liste des invités et le module Conversation dans Connect Pro Central.

Connectez-vous à Connect Pro Central en tant qu'administrateur. Sélectionnez Administration > Conformité et contrôle > Gestion des modules. Décochez l'option pour désactiver la liste des invités et le module Conversation.

Configuration de Live Communications Server 2005

***Remarque :** si vous installez Office Communications Server 2007, consultez « Configuration d'Office Communications Server 2007 » à la page 67.*

1 Sélectionnez Démarrer > Programmes > Outils d'administration > Live Communications Server 2005 pour ouvrir la Console de configuration.

2 Cliquez avec le bouton droit sur la forêt, sélectionnez Propriétés, et procédez comme suit :

a Sélectionnez l'onglet Fédération.

b Activez la case à cocher Activer la connectivité IM publique et de fédération.

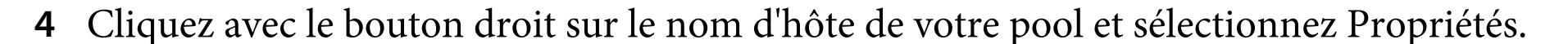
c Entrez l'adresse réseau de Connect Pro.

d Entrez le port 5072.

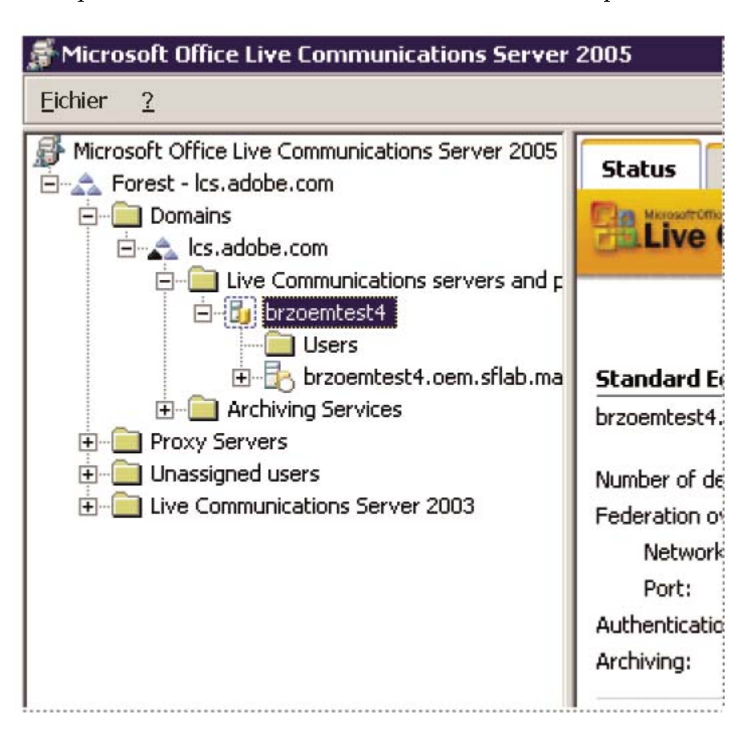
5072 est le numéro de port par défaut de Connect Pro Presence Service dans le fichier \presserv\conf\lcsgw.xml.

e Cliquez sur OK.

3 Dans le volet gauche de la Console de configuration, développez Domaines, développez votre domaine, puis développez les serveurs et les pools Live Communications.



4 Cliquez avec le bouton droit sur le nom d'hôte de votre pool et sélectionnez Propriétés.



5 Dans la boîte de dialogue Propriétés du serveur, procédez comme suit :

a Sélectionnez l'onglet Autorisation d'hôte. Ajoutez l'adresse IP de Connect Pro. Vérifiez que Sortant uniquement a la valeur Non, que Accélérer comme serveur a la valeur Oui, et que Traiter comme authentification a la valeur Oui.

b Si un équilibreur de charge est installé devant votre serveur Connect Pro, ajoutez son adresse IP.

c Cliquez sur OK.

6 Dans le volet gauche de la Console de configuration, développez le nom de domaine pleinement qualifié (FQDN) de votre serveur et sélectionnez Applications.

7 Effectuez les opérations suivantes :

a Cliquez sur Paramétrage de l'application de filtre URL IM. Dans la boîte de dialogue Propriétés, désactivez l'option Activer. Si cette option est activée, les hôtes de réunion ne peuvent pas envoyer d'URL dans des messages instantanés.

8 Fermez la Console de configuration.

Configuration d’Office Communications Server 2007

Remarque : *si vous installez Live Communications Server 2005, consultez « Configuration de Live Communications Server 2005 » à la page 66.*

1 Sélectionnez Démarrer > Programmes > Outils d’administration > Office Communications Server 2007 pour ouvrir la Console de configuration.

2 Cliquez avec le bouton droit sur la forêt, sélectionnez Propriétés, puis Propriétés globales.

3 Sélectionnez l’onglet Général, ajoutez ou sélectionnez un domaine par défaut, puis cliquez sur OK.

4 Sélectionnez l’onglet Fédération, puis procédez comme suit :

a Activez la case à cocher Activer la connectivité IM publique et de fédération.

b Saisissez le nom de domaine pleinement qualifié d’Office Communications Server 2007.

c Entrez le port 5072.

5072 est le numéro de port par défaut de Connect Pro Presence Service dans le fichier \presserv\conf\lcsgw.xml.

d Cliquez sur OK.

5 Dans la forêt, cliquez avec le bouton droit sur le nom de l’hôte, sélectionnez Propriétés, puis Propriétés du serveur frontal.

6 Sélectionnez l’onglet Authentification, choisissez le protocole d’authentification NTLM, puis cliquez sur OK.

7 Sélectionnez l’onglet Authentification de l’hôte, puis procédez comme suit :

a Ajoutez l’adresse IP du système Connect Pro.

b Cochez les cases Accélérer en tant que serveur et Considérer comme authentifié.

c Cliquez sur OK.

8 Cliquez avec le bouton droit sur le nom d’hôte et le nom de domaine (par exemple, brzoemtest5.oem.sflab.macromedia.com) et sélectionnez Propriétés > Propriétés du serveur frontal.

9 Sélectionnez l’onglet Général, puis procédez comme suit :

a Dans la zone Ajouter un port, sélectionnez le port 5072, puis le type de transport TCP et l'option d'envoi à tous les destinataires.

b Dans la zone Ajouter un port, sélectionnez le port 5060, puis le type de transport MTLS et l'option d'envoi à tous les destinataires.

c Dans la zone Ajouter un port, sélectionnez le port 5061, puis le type de transport MTLS et l'option d'envoi à tous les destinataires.

d Activez les trois ports, puis cliquez sur OK.

10 Sélectionnez l’onglet Conférence par messagerie instantanée, puis procédez comme suit :

a Définissez l’adresse IP sur l’adresse du serveur Office Communications Server.

b Définissez le port d’écoute SIP sur 5062.

c Cliquez sur OK.

11 Sélectionnez l’onglet Téléconférence, puis procédez comme suit :

a Définissez l'adresse IP sur l'adresse du serveur Office Communications Server.

b Définissez le port d’écoute SIP sur 5064.

c Cliquez sur OK.

12 Sélectionnez l’onglet Certificats.

Vous affichez les informations concernant votre certificat SSL.

13 Dans la forêt, développez le nom d’hôte et le nom de domaine (par exemple, brzoemtest5.oem.sflab.macromedia.com) et effectuez les opérations suivantes :

a Cliquez avec le bouton droit sur Applications et sélectionnez Propriétés.

b Veillez à ce que la case Intelligent IM URL Filter Application Setting ne soit pas cochée, puis cliquez sur OK.

14 Fermez la Console de configuration.

15 Si vous effectuez une mise à niveau depuis Live Communications Server 2005, effectuez les opérations suivantes :

a Sélectionnez Démarrer > Programmes > Outils d'administration > Utilisateurs et ordinateurs Active Directory.

b Cliquez avec le bouton droit sur le nom d'un utilisateur et sélectionnez Propriétés.

c Sélectionnez l'onglet Communications, puis cliquez sur Configurer (à côté du contrôle Options supplémentaires.)

d Cochez la case Activer la présence enrichie, puis cliquez sur OK.

Configuration des clients du serveur de communication

L'intégration de Connect Pro à des serveurs de communication Microsoft fonctionne avec des clients Microsoft Office Communicator 2005 (MOC 2005) standard. Les clients ne nécessitent aucune configuration particulière. Toutefois, pour pouvoir cliquer sur les URL Connect Meeting dans MOC 2005, modifiez la propriété « Autoriser les liens hypertexte dans les messages instantanés » du modèle Administration du communicateur. Pour plus d'informations, visitez http://technet.microsoft.com/fr-fr/library/bb963959.aspx.

1 Sélectionnez Démarrer > Exécuter.

2 Entrez gpedit.msc dans la zone Ouvrir pour ouvrir la fenêtre Stratégie de groupe.

3 Cliquez pour développer Configuration de l'ordinateur.

4 Cliquez pour développer Modèles d'administration.

5 Cliquez avec le bouton droit sur Paramètres de la stratégie de Microsoft Office Communicator et choisissez Propriétés.

***Remarque :** si le modèle Paramètres de la stratégie de Microsoft Office Communicator n'apparaît pas dans le dossier Modèles d'administration, ajoutez-le. Localisez Communicator.adm dans le package client Microsoft Office Communicator 2005 et copiez-le sous C:\WINDOWS\inf\. Dans la fenêtre Stratégie de groupe, cliquez avec le bouton droit sur Modèles d'administration, cliquez sur Ajouter/Supprimer des modèles, puis sur Ajouter, accédez au fichier, puis cliquez sur Ouvrir.*

Configuration de Connect Pro Presence Service

Effectuez les quatre procédures suivantes pour configurer Connect Pro Presence Service pour échanger des données avec un serveur de communication. Une fois la configuration terminée, redémarrez Connect Pro Central Application Server.

Définition de la connexion de passerelle entre Connect Pro Presence Service et le serveur de communication

1 Ouvrez le fichier *RootInstallationFolder*\presserv\conf\lcsgw.xml dans un éditeur XML.

2 Modifiez le fichier comme suit en remplaçant vos valeurs par celles en gras :

```
<?xml version="1.0" encoding="UTF-8"?>
<config>
<block xmlns="accept:config:sip-lcsgw">
<service trace="off" name="lcsgw" id="internal.server">
<stack name="lcs">
<via/>
</stack>
<state type="enabled"/>
<host type="external">lcs.adobe.com</host>
<domain-validation state="false"/>
<binding name="connector-0" transport="tcp">
<port>5072</port>
<bind>10.59.72.86</bind> <!-- LCS server IP -->
<area>lcs.adobe.com</area> <!-- LCS domain -->
</binding>
</service>
</block>
</config>
```

Paramètre	Description
`<hôte>`	Domaine SIP des utilisateurs LCS ou OCS
`<bind>`	Adresse IP du serveur LCS ou OCS (ou de l'équilibreur de charge
`<area>`	Domaine SIP des utilisateurs LCS ou OCS

Configuration du fichier custom.ini.

1 Ouvrez *RootInstallationFolder*\custom.ini dans un éditeur de texte.

2 Entrez les paramètres et valeurs ci-dessous :

Paramètre	Valeur
OPN_ADAPTOR	com.macromedia.breeze.opn.OPNGateway Cette valeur respecte la casse.
OPN_HOST	Adresse réseau de Connect Pro Presence Service (par exemple, localhost).
OPN_PORT	Port interne utilisé entre Connect Pro et Connect Pro Presence Service. La valeur par défaut (10020) doit correspondre à la valeur du fichier *RootInstallationFolder*\presserv\conf\router.xml. Ne modifiez pas cette valeur.
OPN_PASSWORD	Jeton interne utilisé entre Connect Pro et Connect Pro Presence Service. La valeur par défaut (secrète) doit correspondre à la valeur du fichier *RootInstallationFolder*\presserv\conf\router.xml. Ne modifiez pas cette valeur.
OPN_DOMAIN	Nom de domaine du serveur Connect Pro (serveur d'applications). Connect Pro Presence Service utilise ce nom pour identifier le serveur d'applications. Dans un cluster, chaque serveur d'applications doit avoir son propre nom de domaine.
MEETING_PRESENCE_POLL_INTERVAL	Les clients hôtes interrogent régulièrement le serveur de présence pour récupérer l'état des invités. Ce paramètre définit le nombre de secondes entre des requêtes d'interrogation. La valeur par défaut est 30. Ne modifiez pas cette valeur.

Exemples de paramètres :

```
OPN_ADAPTOR=com.macromedia.breeze.opn.OPNGateway
OPN_HOST=localhost
OPN_PORT=10020
OPN_PASSWORD=secret
OPN_DOMAIN=breeze01.com
```

Définition de la passerelle SIP vers Connect Pro Presence Service

1 Ouvrez le fichier *RootInstallationFolder*\presserv\conf\router.xml dans un éditeur XML.

2 Modifiez le fichier comme suit en remplaçant vos valeurs par celles en gras :

```
<block xmlns="accept:config:xmpp-gateway">
...
<block xmlns="accept:config:sip-stack-manager">
<service trace="off">
<bind>10.133.192.75</bind> <!-- presence server machine IP -->
<state type="enabled"/></service></block>
```

Dans la balise `<bind>`, entrez l'adresse IP de l'ordinateur qui héberge Connect Pro. Si plusieurs adresses IP sont renvoyées, sélectionnez l'adresse IP interne ou externe que le serveur LCS ou OCS distant peut résoudre pour se connecter à Connect Pro.

3 Redémarrez Connect Pro Central Application Server.

Configuration de Connect Pro Presence Service dans un cluster

Si vous exécutez Connect Pro dans un cluster, exécutez Connect Pro Presence Service sur un seul ordinateur du cluster. Veillez cependant à configurer Connect Pro Presence Service sur tous les ordinateurs du cluster de manière à permettre l'échange du trafic de présence.

1 Ouvrez le fichier *[rép_install_racine]*\custom.ini dans un éditeur de texte.

2 Entrez les paramètres et valeurs ci-dessous :

Paramètre	Valeur
OPN_ADAPTOR	com.macromedia.breeze.opn.OPNGateway Cette valeur respecte la casse.
OPN_HOST	Nom de domaine pleinement qualifié de l'ordinateur qui exécute Connect Pro Presence Service. La valeur du paramètre OPN_HOST est la même sur chaque ordinateur d'un cluster.
OPN_PORT	Port interne utilisé entre Connect Pro et Connect Pro Presence Service. La valeur par défaut (10020) doit correspondre à la valeur du fichier *RootInstallationFolder*\presserv\conf\router.xml. Ne modifiez pas cette valeur.
OPN_PASSWORD	Jeton interne utilisé entre Connect Pro et Connect Pro Presence Service. La valeur par défaut (secrète) doit correspondre à la valeur du fichier *RootInstallationFolder*\presserv\conf\router.xml. Ne modifiez pas cette valeur.
OPN_DOMAIN	Domaine qu'utilise Connect Pro Presence Service pour identifier un serveur Connect Pro dans un cluster. Chaque ordinateur d'un cluster doit avoir une valeur unique. Le paramètre OPN_DOMAIN peut avoir une valeur quelconque (par exemple, presence.connect1, presence.connect2, connect3) pour autant qu'elle soit unique dans le cluster.
MEETING_PRESENCE_POLL_INTERVAL	Les clients hôtes interrogent régulièrement le serveur de présence pour récupérer l'état des invités. Ce paramètre définit le nombre de secondes entre des requêtes d'interrogation. La valeur par défaut est 30. Ne modifiez pas cette valeur.

Exemples de paramètres :

```
OPN_ADAPTOR=com.macromedia.breeze.opn.OPNGateway
OPN_HOST=localhost
OPN_PORT=10020
OPN_PASSWORD=secret
OPN_DOMAIN=presence.connect1
```

3 Redémarrez Connect Pro Central Application Server.

Démarrage et arrêt de Connect Pro Presence Service

Vous pouvez arrêter et démarrer Connect Pro Presence Service dans le menu Démarrer ou dans la fenêtre Services.

Démarrage et arrêt de Connect Pro Presence Service via le menu Démarrer

❖ Effectuez l'une des opérations suivantes :

- Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server > Démarrer Connect Pro Presence Service.
- Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server > Arrêter Connect Pro Presence Service.

Démarrage et arrêt de Connect Pro Presence Service via la fenêtre Services

1 Choisissez Démarrer > Panneau de configuration > Outils d'administration > Services pour ouvrir la fenêtre Services.

2 Sélectionnez Connect Pro Presence Service et cliquez sur Démarrer le service, Arrêter le service ou Redémarrer le service.

Configuration de l'authentification unique

A propos de l'authentification unique

L'authentification unique est un mécanisme qui authentifie les utilisateurs pour toutes les applications pour lesquelles ils disposent de droits d'accès sur un réseau. L'authentification unique utilise un serveur proxy pour authentifier les utilisateurs afin qu'ils ne doivent pas ouvrir de session dans Connect Pro.

Connect Pro prend en charge les mécanismes d'authentification uniques suivants :

Authentification des en-têtes HTTP Configurez un proxy d'authentification pour intercepter la requête HTTP, analysez les informations de connexion de l'utilisateur dans l'en-tête et transmettez-les à Connect Pro.

Authentification NTLM (Microsoft NT LAN Manager) Configurez Connect Pro pour qu'il tente d'authentifier automatiquement la connexion des clients par rapport à un contrôleur de domaine Windows utilisant le protocole NTLMv1. Microsoft Internet Explorer sous Microsoft Windows peut négocier une authentification NTLM sans demander ses informations de connexion à l'utilisateur.

Remarque : *L'authentification NTLM ne fonctionne pas sur les serveurs Edge. Utilisez plutôt l'authentification LDAP.*

Remarque : *il se peut que les clients Mozilla Firefox puissent négocier une authentification NTLM sans la demander. Pour plus d'informations sur la configuration, consultez ce document Firefox.*

Vous pouvez également écrire votre propre filtre d'authentification. Pour plus d'informations, contactez l'assistance technique d'Adobe.

Configuration de l'authentification des en-têtes HTTP

Lorsque l'authentification des en-têtes HTTP est configurée, les requêtes de connexion à Connect Pro sont acheminées vers un agent placé entre le client et Connect Pro. Cet agent peut être un proxy d'authentification ou une application logicielle qui authentifie l'utilisateur, ajoute un autre en-tête dans la requête HTTP et envoie celle-ci à Connect Pro. Sur Connect Pro, vous devez retirer le commentaire d'un filtre Java et configurer un paramètre du fichier custom.ini qui indique le nom de l'en-tête HTTP supplémentaire.

Voir aussi

« Démarrage et arrêt de Connect Pro » à la page 103

Configuration d'une authentification des en-têtes HTTP sur Connect Pro

Pour activer l'authentification des en-têtes HTTP, configurez le mappage d'un filtre Java et un paramètre d'en-tête sur l'ordinateur qui héberge Connect Pro.

1 Ouvrez le fichier *[rép_install_racine]*\TelephonyService\conf\WEB-INF\web.xml et procédez comme suit :

a Retirez les commentaires du mappage du filtre Java HeaderAuthenticationFilter.

```
<filter-mapping>
    <filter-name>HeaderAuthenticationFilter</filter-name>
    <url-pattern>/*</url-pattern>
</filter-mapping>
```

b Appliquez un commentaire au mappage du filtre Java NtlmAuthenticationFilter.

```
<!--
<filter-mapping>
    <filter-name>NtlmAuthenticationFilter</filter-name>
    <url-pattern>/*</url-pattern>
</filter-mapping>
-->
```

2 Arrêtez·Connect Pro :

a Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server > Arrêter Connect Pro Central Application Server.

b Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server > Arrêter Connect Pro Meeting Server.

3 Ajoutez la ligne suivante dans le fichier custom.ini :

```
HTTP_AUTH_HEADER=header_field_name
```

Votre agent d'authentification doit ajouter un en-tête à la requête HTTP envoyée à Connect Pro. Le nom de l'en-tête doit être `header_field_name`.

4 Enregistrez le fichier custom.ini et redémarrez Connect Pro.

a Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server > Démarrer Connect Pro Meeting Server.

b Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server > Démarrer Connect Pro Central Application Server.

Rédaction du code d'authentification

Le code d'authentification doit authentifier l'utilisateur, ajouter un champ dans l'en-tête HTTP contenant le nom d'utilisateur et envoyer une requête à Connect Pro.

1 Sélectionnez la valeur du champ d'en-tête *header_field_name* pour une connexion utilisateur à Connect Pro.

2 Envoyez une requête HTTP à Connect Pro à l'adresse URL suivante :

```
http://connectURL/system/login
```

Le filtre Java sur Connect Pro intercepte la requête, recherche l'en-tête *header_field_name*, puis recherche un utilisateur avec l'ID transmis dans l'en-tête. Si l'utilisateur est localisé, il est authentifié et une réponse est envoyée.

3 Dans le contenu HTTP de la réponse de Connect Pro, recherchez la chaîne `"OK"` qui indique une authentification réussie.

4 Dans la réponse de Connect Pro, recherchez le cookie `BREEZESESSION`.

5 Redirigez l'utilisateur vers l'URL requise sur Connect Pro et transmettez le cookie `BREEZESESSION` représentant la valeur du paramètre `session`, comme suit :

```
http://connectURL?session=BREEZESESSION
```

Remarque : *vous devez transmettre le cookie `BREEZESESSION` dans toute requête ultérieure à Connect Pro au cours de la session client.*

Configuration de l'authentification des en-têtes HTTP avec Apache

La procédure suivante décrit un exemple d'implémentation de l'authentification des en-têtes HTTP qui utilise Apache comme agent d'authentification.

1 Installez Apache en tant que proxy inverse sur un autre ordinateur que celui qui héberge Connect Pro.

2 Choisissez Démarrer > Programmes > Apache HTTP Server > Configure Apache Server > Edit the Apache httpd.conf Configuration file. Effectuez ensuite les opérations suivantes :

a Retirez les commentaires de la ligne suivante :

```
LoadModule headers_module modules/mod_headers.so
```

b Retirez les commentaires des trois lignes suivantes :

```
LoadModule proxy_module modules/mod_proxy.so
LoadModule proxy_connect_module modules/mod_proxy_connect.so
LoadModule proxy_http_module modules/mod_proxy_http.so
```

c Ajoutez les lignes suivantes à la fin du fichier :

```
RequestHeader append custom-auth "ext-login"
ProxyRequests Off
<Proxy *>
Order deny,allow
Allow from all
</Proxy>
ProxyPass / http://hostname:[port]/
ProxyPassReverse / http://hostname:[port]/
ProxyPreserveHost On
```

3 Arrêtez·Connect Pro :

a Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server > Arrêter Connect Pro Central Application Server.

b Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server > Arrêter Connect Pro Meeting Server.

4 Sur l'ordinateur qui héberge Connect Pro, ajoutez les lignes de code suivantes dans le fichier custom.ini (situé dans le répertoire racine d'installation, c:\breeze par défaut) :

```
HTTP_AUTH_HEADER=custom-auth
```

Le paramètre `HTTP_AUTH_HEADER` doit correspondre au nom configuré sur le serveur proxy. (Dans cet exemple, il a été configuré à la ligne 1 de l'étape 2c.) Le paramètre correspond à l'en-tête HTTP supplémentaire.

5 Enregistrez le fichier custom.ini et redémarrez Connect Pro.

a Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server > Démarrer Connect Pro Meeting Server.

b Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server > Démarrer Connect Pro Central Application Server.

6 Ouvrez le fichier *[rép_install_racine]*\TelephonyService\conf\WEB-INF\web.xml et procédez comme suit :

a Retirez les commentaires du mappage du filtre Java HeaderAuthenticationFilter.

```
<filter-mapping>
    <filter-name>HeaderAuthenticationFilter</filter-name>
    <url-pattern>/*</url-pattern>
</filter-mapping>
```

b Appliquez un commentaire au mappage du filtre Java NtlmAuthenticationFilter.

```
<!--
<filter-mapping>
    <filter-name>NtlmAuthenticationFilter</filter-name>
    <url-pattern>/*</url-pattern>
</filter-mapping>
-->
```

Configuration de l'authentification NTLM

NTLMv1 est un protocole d'authentification utilisé avec le protocole de réseau SMB sur les réseaux Microsoft Windows. Vous pouvez utiliser NTLM pour permettre à un utilisateur de prouver son identité sur un domaine Windows une fois puis l'autoriser à accéder à une autre ressource de réseau, comme Connect Pro. Pour créer les informations de connexion de l'utilisateur, le navigateur Web de l'utilisateur exécute automatiquement une authentification de défi et de réponse avec le contrôleur de domaine via Connect Pro. Si ce mécanisme échoue, l'utilisateur peut se connecter directement à Connect Pro. Seul Internet Explorer sur Windows prend en charge la connexion unique avec une authentification NTLMv1.

Remarque : *par défaut, les contrôleurs de domaine Windows Server 2003 nécessitent une fonction de sécurité appelée signatures SMB. Les signatures SMB ne sont pas prises en charge par la configuration par défaut du filtre d'authentification NTLM. Vous pouvez configurer le filtre pour fonctionner sous cette condition. Pour plus d'informations sur cette option et sur d'autres options de configuration avancées, consultez la documentation d'authentification JCIFS NTLM HTTP.*

Ajout de paramètres de configuration

Procédez comme suit pour chaque hôte du cluster Connect Pro :

1 Ouvrez le fichier *[rép_install_racine]*\custom.ini dans un éditeur de texte et ajoutez les paramètres suivants :

```
NTLM_DOMAIN=[domain]
NTLM_SERVER=[WINS_server_IP_address]
```

La valeur `[domain]` correspond au nom du domaine Windows dont les utilisateurs sont des membres et avec lequel ils s'authentifient, par exemple, CORPNET. Vous devrez peut-être paramétrer cette valeur sur la version du nom de domaine compatible avec les versions antérieures à Windows 2000. Pour plus d'informations, consultez TechNote 27e73404. Cette valeur est mappée sur la propriété de filtre `jcifs.smb.client.domain`. Définir directement la valeur dans le fichier web.xml remplace la valeur figurant dans le fichier custom.ini.

La valeur `[WINS_server_IP_address]` est l'adresse IP ou une liste d'adresses IP de serveurs WINS séparées par des virgules. Utilisez l'adresse IP, le nom d'hôte ne fonctionne pas. Les serveurs WINS sont interrogés dans l'ordre spécifié pour résoudre l'adresse IP d'un contrôleur de domaine pour le domaine spécifié dans le paramètre `NTLM_DOMAIN`. (Le contrôleur de domaine authentifie ses utilisateurs.) Vous pouvez également spécifier l'adresse IP du contrôleur de domaine lui-même, par exemple, 10.169.10.77, 10.169.10.66. Cette valeur est mappée vers la propriété de filtre `jcifs.netbios.wins`. Définir la valeur dans le fichier web.xml remplace la valeur figurant dans le fichier custom.ini.

2 Enregistrez le fichier custom.ini.

3 Ouvrez le fichier *[rép_install_racine]*\TelephonyService\conf\WEB-INF\web.xml dans un éditeur de texte et procédez comme suit :

a Supprimez les commentaires du mappage NtlmAuthenticationFilter mapping pour qu'il prenne l'aspect suivant :

```
<filter-mapping>
    <filter-name>NtlmAuthenticationFilter</filter-name>
    <url-pattern>/*</url-pattern>
</filter-mapping>
```

b Commentez le mappage de filtre HeaderAuthenticationFilter pour qu'il prenne l'aspect suivant :

```
<!--
<filter-mapping>
    <filter-name>HeaderAuthenticationFilter</filter-name>
    <url-pattern>/*</url-pattern>
</filter-mapping>
-->
```

4 Enregistrez le fichier web.xml.

5 Redémarrez Connect Pro.

a Sélectionnez Démarrer > Tous les programmes > Adobe Acrobat Connect Pro Server > Arrêter Adobe Acrobat Connect Pro Server.

b Sélectionnez Démarrer > Tous les programmes > Adobe Acrobat Connect Pro Server > Démarrer Adobe Acrobat Connect Pro Server.

Rapprochement des stratégies de connexion

Les stratégies de connexion de Connect Pro et NTLM diffèrent quant à l'authentification des utilisateurs. Conciliez ces stratégies avant que les utilisateurs puissent employer une seule connexion.

L'identifiant de connexion utilisé par le protocole NTLM peut être un nom d'utilisateur (jdoe), un numéro d'employé (1234) ou un nom codé, selon la stratégie ou l'organisation. Par défaut, Connect Pro utilise une adresse électronique (jdoe@masociete.com) comme identifiant de connexion. Modifiez la stratégie de connexion à Connect Pro pour que Connect Pro partage un identifiant unique avec NTLM.

1 Ouvrez Connect Pro Central.

Pour ouvrir Connect Pro Central, ouvrez une fenêtre de navigateur, puis entrez le nom de domaine pleinement qualifié de l’hôte Connect Pro (par exemple http://connect.masociété.com). Entrez la valeur de l'hôte Connect Pro dans l'écran Paramètres du serveur de la Console de gestion des applications.

2 Sélectionnez l’onglet Administration. Cliquez sur Utilisateurs et groupes. Cliquez sur Modifier les stratégies de nom d'utilisateur et de mot de passe.

3 Dans la section Stratégie de connexion, sélectionnez Non pour Utiliser l'adresse de messagerie comme identifiant de connexion.

Configuration d'un proxy inverse devant Connect Pro

Utilisation d'un proxy inverse

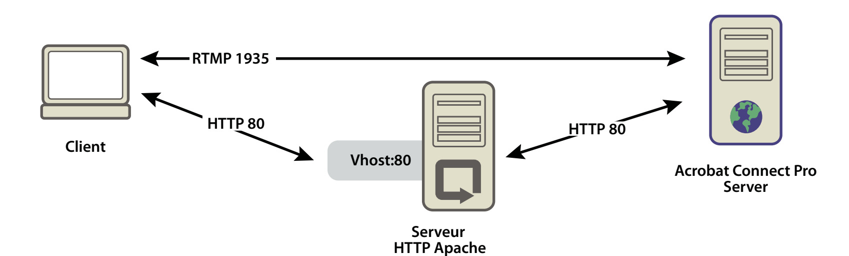
Vous pouvez configurer un proxy inverse devant Connect Pro. Le trafic circule via le proxy inverse avant d'atteindre Connect Pro. Procédez comme suit à l'aide de cette configuration :

- Laissez Connect Pro à l'extérieur du DMZ.

  Placez le proxy inverse dans le DMZ et placez Connect Pro derrière le pare-feu de votre organisation.

- Authentifiez les utilisateurs avant qu'ils atteignent Connect Pro.

  Le proxy inverse authentifie les utilisateurs avec un autre système et les autorise à se connecter à Connect Pro.



Le trafic HTTP est diffusé via Apache HTTP Server pour rejoindre Connect Pro.

Configuration d'un proxy inverse

Cet exemple est basé sur l'installation Windows (32 bits) d'Apache HTTP Server. La configuration est identique sur tous les systèmes d'exploitation pris en charge par Apache. Cet exemple n'utilise pas SSL : le trafic vers le serveur d'application Connect Pro n'est pas codé.

Procédez comme suit pour forcer le trafic HTTP à circuler via Apache HTTP Server avant d'atteindre Connect Pro :

Remarque : *le trafic RTMP ne circule pas via Apache HTTP Server dans cette configuration.*

1 Installez Apache HTTP Server.

Par défaut, les fichiers de configuration Apache sont situés dans le dossier c:\Program Files\Apache Software Foundation\Apache2.2\conf\.

2 Configurez Apache pour qu'il écoute l'ensemble du trafic sur le port 80.

Ouvrez le fichier c:\Program Files\Apache Software Foundation\Apache2.2\conf\httpd.conf dans un éditeur de texte et ajoutez ce qui suit :

```
#
# Listen: Allows you to bind Apache to specific IP addresses and
# ports, instead of the default. See also the <VirtualHost>
# directive.
#
# Change this to Listen on specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses.
#
#Listen 12.34.56.78:80
Listen 80
#
#
```

3 Chargez les modules requis pour le fonctionnement en tant que proxy inverse.

Dans le même fichier (httpd.conf), supprimez les commentaires des lignes suivantes :

```
LoadModule proxy_module modules/mod_proxy.so
LoadModule proxy_http_module modules/mod_proxy_http.so
LoadModule proxy_connect_module modules/mod_proxy_connect.so
```

4 Liez le fichier httpd.conf au fichier de configuration qui dirige les connexions vers Connect Pro.

Ajoutez la ligne suivante à la dernière ligne du fichier httpd.conf :

```
Include conf/extra/httpd-connect.conf
```

5 Créez un fichier texte appelé httpd-connect.conf et enregistrez-le sur le chemin d'accès suivant : c:\Program Files\Apache Software Foundation\Apache2.2\conf\extra.

6 Ajoutez les lignes suivantes au fichier httpd-connect.conf (insérez vos adresses IP et les ports à l'endroit demandé) :

```
#vhost for application server
<VirtualHost *:80>
ProxyRequests Off
ProxyPreserveHost On
ProxyPass / http://<IP-of-Connect-Application-Server>:80/
ProxyPassReverse / http://<IP-of-Connect-Application-Server>:80/
ServerName <FQDN of Apache host>
</VirtualHost>
```

7 Enregistrez le fichier et relancez le service Apache.

8 Ouvrez la Console de gestion des applications de Connect Pro dans un navigateur : http://localhost:8510/console/

9 Sur l'écran des paramètres du serveur, procédez comme suit :

- Paramétrez l'hôte Connect Pro sur le nom de domaine pleinement qualifié d'Apache HTTP Server.
- Paramétrez le nom externe sur le nom de domaine pleinement qualifié de l'ordinateur hébergeant Connect Meeting Server.

10 Relancez le service Connect Pro (le serveur d'application) et le service Flash Media Server (FMS) (le serveur de réunion). Voir « Démarrage et arrêt des serveurs » à la page 103.

RTMP est dirigé vers Connect Pro et HTTP est dirigé via Apache.

Hébergement d'Acrobat Connect Add-in

Présentation d'Acrobat Connect Add-in

L'application Adobe Acrobat Connect Add-in est une version de Flash Player qui comprend des fonctionnalités avancées pour les réunions Acrobat Connect Pro.

Lorsqu'Acrobat Connect Add-in est nécessaire, il est téléchargé depuis un serveur Adobe par un processus transparent que l'utilisateur ne voit pas. Toutefois, si votre société n'autorise pas ses employés à télécharger des logiciels à partir de serveurs externes, vous pouvez héberger Acrobat Connect Add-in sur votre propre serveur.

Les invités aux réunions, les utilisateurs inscrits et les présentateurs sont invités à télécharger Acrobat Connect Add-in lorsqu'une ancienne version est installée sur leur ordinateur et qu'ils sont promus hôte ou présentateur ou que des droits étendus leur sont accordés pour le module Partage.

Les hôtes de réunion doivent obligatoirement télécharger Acrobat Connect Add-in lorsqu'il n'est pas installé ou pour remplacer une ancienne version.

Personnalisation de l'emplacement de téléchargement d'Acrobat Connect Add-in

Vous pouvez héberger Acrobat Connect Add-in sur votre serveur et envoyer directement les utilisateurs vers les fichiers exécutables. Vous pouvez également diriger les utilisateurs vers une page d'instructions de téléchargement contenant des liens vers les fichiers exécutables. Vous pouvez créer votre propre page d'instructions de téléchargement ou utiliser celle fournie par Adobe. La page d'Adobe est traduite dans toutes les langues prises en charge.

Envoyez directement les utilisateurs vers les fichiers exécutables.

1 Recherchez les fichiers de langue XML Connect Pro sur le serveur hébergeant Acrobat Connect Pro. Les fichiers XML se trouvent dans les deux répertoires suivants :*[rép_install_racine]*\appserv\web\common\intro\lang et *[rép_install_racine]*\appserv\web\common\meeting\lang\.

2 Entrez un chemin aux fichiers exécutable pour chaque plate-forme dans la section `addInLocation` de chaque plate-forme dans chaque fichier de langue :

```
<m id="addInLocation" platform="Mac OS 10">/common/addin/AcrobatConnectAddin.z</m>
<m id="addInLocation" platform="Windows">/common/addin/setup.exe</m>
```

Remarque : *il s'agit là des emplacements par défaut des fichiers exécutables de l'Add-in. Vous pouvez modifier les emplacements sur le serveur et changer en conséquence les chemins d'accès dans la section* `addInLocation`.

Envoyez les utilisateurs vers les pages d'instructions de téléchargement fournies par Adobe.

1 Recherchez les fichiers de langue XML Connect Pro sur le serveur hébergeant Connect Pro. Les fichiers XML se trouvent dans les deux répertoires suivants :*[rép_install_racine]*\appserv\web\common\intro\lang et *[rép_install_racine]*\appserv\web\common\meeting\lang\.

2 Entrez le chemin à la page d'instructions de téléchargement dans la section `addInLocation` de chaque plate-forme dans chaque fichier de langue :

```
<m id="addInLocation" platform="Mac OS 10">/common/help/#lang#/support/addindownload.htm</m>
<m id="addInLocation" platform="Windows">/common/help/#lang#/support/addindownload.htm</m>
```

Remarque : *Le chemin comprend une chaîne* `#lang#` *que Connect Pro traduit dans la langue de la réunion au moment de l'exécution.*

3 Le fichier addindownload.htm comprend des liens vers les emplacements par défaut des fichiers exécutables de l'Add-in sur Connect Pro (/common/addin/setup.exe et /common/addin/AcrobatConnectAddin.z). Si vous modifiez l'emplacement des fichiers exécutables, actualisez les liens de la page addindownload.htm pour chaque langue.

Envoyez les utilisateurs vers vos propres pages d'instructions de téléchargement.

1 Recherchez les fichiers de langue XML Connect Pro sur le serveur hébergeant Connect Pro. Les fichiers XML se trouvent dans les deux répertoires suivants :*[rép_install_racine]*\appserv\web\common\intro\lang et *[rép_install_racine]*\appserv\web\common\meeting\lang\.

2 Dans la section `addInLocation` de chaque plate-forme dans chaque fichier de langue, entrez le chemin à la page d'instructions que vous avez créée :

```
<m id="addInLocation" platform="Mac OS
10">common/help/#lang#/support/addin_install_instructions.html</m>
<m id="addInLocation"
platform="Windows">common/help/#lang#/support/addin_install_instructions.html</m>
```

Remarque : *vous pouvez créer des pages d'instructions distinctes pour chaque plate-forme.*

3 Créez une page d'instruction pour chaque langue que vous désirez prendre en charge. Dans la page d'instructions, ajoutez des liens vers les fichiers exécutables de l'Add-in pour chaque plate-forme.

Chapitre 4 : Stratégies

La sécurisation d'Adobe® Connect™ protège votre société contre les pertes de biens et les actes de malveillance. Il est important de sécuriser l'infrastructure de votre société, Acrobat Connect Pro Server et le serveur de base de données utilisé par Acrobat Connect Pro Server.

Protocole SSL (Secure Sockets Layer)

A propos de la prise en charge SSL

Acrobat Connect Pro Server est constitué de deux serveurs : Adobe® Flash® Media Server et le serveur d'applications Acrobat Connect Pro. Flash Media Server est appelé « *serveur de réunions* » car il permet au client d'accéder aux réunions via une connexion RTMP en temps réel. Le serveur d'applications Acrobat Connect Pro gère la connexion HTTP entre le client et la logique applicative d'Acrobat Connect Pro.

Remarque : *dans le menu Démarrer, le serveur de réunions est appelé « Connect Pro Meeting Server » et le serveur d'applications « Connect Pro Central Application Server ». Dans la fenêtre Services, le serveur de réunions est appelé « Flash Media Server (FMS) » et le serveur d'applications « Adobe Connect Enterprise Service ».*

Vous pouvez configurer SSL pour le serveur d'applications, pour le serveur de réunions, ou pour les deux :

Solution matérielle Pour obtenir une configuration SSL la plus fiable possible, utilisez un accélérateur SSL.

Achetez un accélérateur SSL séparément. Adobe a vérifié le fonctionnement d'Acrobat Connect Pro avec les accélérateurs matériels SSL suivants : F5 Big-IP 1000, Cisco Catalyst 6590 Switch et Radware T100.

Solution logicielle Utilisez la prise en charge native de SSL dans Acrobat Connect Pro.

Remarque : *SSL n'est pas pris en charge sous Microsoft® Windows® 98.*

Acrobat Connect Pro utilise la méthode HTTP `CONNECT` pour demander une connexion SSL. Les serveurs proxy doivent autoriser les clients à utiliser la méthode `CONNECT`. Si les clients ne peuvent pas utiliser la méthode `CONNECT`, les connexions RTMP passent par HTTP/HTTPS.

Pour obtenir de l'aide sur la configuration de SSL, contactez l'assistance technique d'Adobe à l'adresse www.adobe.com/go/connect_licensed_programs_fr.

Utilisation de certificats

Un certificat SSL vérifie l'identité du serveur sur le client.

Pour sécuriser les connexions des serveurs de réunions (RTMP) et d'applications (HTTP), vous devez disposer de deux certificats SSL, un pour chaque connexion. Pour configurer SSL pour un cluster d'ordinateurs qui hébergent Acrobat Connect Pro, vous devez avoir un certificat SSL pour chaque serveur de réunions. Tous les serveurs d'applications d'un cluster peuvent partager un même certificat SSL.

Par exemple, pour sécuriser la connexion à un serveur de réunions et à des serveurs d'applications sur un serveur, vous avez besoin au total de deux certificats SSL. Pour sécuriser la connexion aux serveurs de réunions et aux serveurs d'applications sur un cluster de trois serveurs, vous avez besoin d'un total de quatre certificats SSL : un partagé par les serveurs d'applications et trois pour les serveurs de réunions.

Obtention de certificats

❖ Contactez une autorité de certification, organisme tiers approuvé qui vérifie l'identité du demandeur. (Les certificats auto-signés ne fonctionnent pas avec Acrobat Connect Pro.)

L'autorité de certification vous invite à générer un fichier CSR (Certificate Signing Request) SSL. Envoyez-le à l'autorité de certification qui le convertira en certificat SSL. Il contient des informations sur votre société et le nom de domaine pleinement qualifié associé au certificat SSL. Pour des instructions précises sur la création d'un fichier CSR, contactez votre autorité de certification.

***Important :** conservez les mots de passe de vos certificats SSL dans un endroit sécurisé et accessible.*

Installation des certificats

❖ Installez les certificats SSL et les fichiers de clé privée au format PEM dans le dossier racine Acrobat Connect Pro (c:\breeze, par défaut).

Si vous recevez un fichier CRT d'une autorité de certification, vous pouvez le renommer en lui donnant l'extension .pem.

***Remarque :** vous devez avoir deux fichiers pour chaque connexion sécurisée, un fichier pour le certificat public et un fichier pour la clé privée. Le serveur envoie le certificat public au client. La clé privée reste sur le serveur.*

Configuration d'un protocole SSL logiciel

Lorsque vous configurez un protocole SSL logiciel, vous pouvez sécuriser le serveur d'applications (HTTP), le serveur de réunions (RTMP) ou les deux. Quelle que soit la configuration que vous choisissez, vous devez d'abord configurer le serveur DNS.

Configuration du serveur DNS

❖ Créez des entrées DNS qui définissent un nom de domaine pleinement qualifié pour chaque connexion sécurisée.

Le nom de domaine pleinement qualifié du serveur d'applications est l'URL avec laquelle les utilisateurs finaux se connectent à Acrobat Connect Pro. Entez ce nom de domaine pleinement qualifié pour la valeur Hôte Connect Pro dans la page Paramètres du serveur de la Console de gestion des applications. « Connect » est un exemple de valeur valide. *votresociété* .com

Les utilisateurs finaux ne voient pas le nom de domaine pleinement qualifié du serveur de réunions. Il est cependant indispensable d'en définir un pour le serveur de réunions si vous souhaitez tenir des réunions via une connexion sécurisée. Entrez le nom de domaine pleinement qualifié dans la zone Nom externe de la page Paramètres du serveur de la Console de gestion des applications. Valeur possible : fms.votresociété.com.

***Remarque :** dans un cluster de serveurs, tous les serveurs d'applications peuvent partager un certificat SSL, mais chaque serveur de réunions doit avoir son propre certificat SSL. Sur un même serveur, pour sécuriser à la fois les connexions HTTP (serveurs d'applications) et RTMP (serveur de réunions), vous devez avoir un total de deux noms de domaine pleinement qualifiés et deux certificats SSL (un pour chaque protocole).*

Sécurisation du serveur de réunions et du serveur d'applications

1 Ouvrez le fichier Adaptor.xml situé dans le dossier *[rép_install_racine]*\comserv\win32\conf_defaultRoot_ et enregistrez une copie de sauvegarde dans un autre emplacement.

2 Insérez le code suivant dans le fichier Adaptor.xml d'origine, à l'intérieur des balises `<Adaptor></Adaptor>` (remplacez le code en italique par vos propres valeurs) :

```
<SSL>
    <Edge name="meetingserver">
        <SSLServerCtx>
<SSLCertificateFile>[root_install_dir]\sslMeetingPublicCert.pem</SSLCertificateFile>
    <SSLCertificateKeyFile
type="PEM">[root_install_dir]\sslMeetingPrivateKey.pem</SSLCertificateKeyFile>
            <SSLPassPhrase>mypassphrase</SSLPassPhrase>
            <SSLCipherSuite>ALL:!ADH:!LOW:!EXP:!MD5:@STRENGTH</SSLCipherSuite>
            <SSLSessionTimeout>5</SSLSessionTimeout>
        </SSLServerCtx>
    </Edge>
    <Edge name="applicationserver">
        <SSLServerCtx>

<SSLCertificateFile>[root_install_dir]\sslAppServerPublicCert.pem</SSLCertificateFile>
            <SSLCertificateKeyFile
type="PEM">[root_install_dir]\sslAppServerPrivateKey.pem</SSLCertificateKeyFile>
            <SSLPassPhrase>mypassphrase</SSLPassPhrase>
            <SSLCipherSuite>ALL:!ADH:!LOW:!EXP:!MD5:@STRENGTH</SSLCipherSuite>
            <SSLSessionTimeout>5</SSLSessionTimeout>
        </SSLServerCtx>
    </Edge>
</SSL>
```

Vous devez avoir deux fichiers pour chaque connexion sécurisée : un pour le certificat SSL public et un pour la clé privée appartenant au certificat. Indiquez l'emplacement du certificat SSL public dans la balise `<SSLCertificateFile>`. Indiquez l'emplacement de la clé privée dans la balise `<SSLCertificateKeyFile>`. Le serveur envoie le certificat SSL public aux clients. La clé privée reste sur le serveur.

3 Localisez la ligne suivante dans le fichier Adaptor.xml :

```
<HostPort name="edge1">${DEFAULT_FCS_HOSTPORT}</HostPort>
```

4 Remplacez le code de l'étape 3 par :

```
<HostPort name="meetingserver" ctl_channel=":19350">meetingServerIP:-443</HostPort>
<HostPort name="applicationserver" ctl_channel=":19351">appServerIP:-443</HostPort>
```

5 Enregistrez le fichier Adaptor.xml.

6 (Facultatif) Ouvrez le fichier Adaptor.xml dans un navigateur Web pour valider sa syntaxe.

Si le navigateur signale une erreur, corrigez-la, puis rouvrez le fichier dans un navigateur Web. Répétez ce processus jusqu'à ce que le fichier soit valide.

7 Ouvrez le fichier custom.ini situé dans le répertoire d'installation racine (c:\breeze, par défaut) et enregistrez une copie de sauvegarde dans un autre emplacement.

8 Insérez le code suivant dans le fichier custom.ini, sans remplacer ni supprimer le texte existant :

```
ADMIN_PROTOCOL=https://
SSL_ONLY=yes
HTTPS_PORT=8443
RTMP_SEQUENCE=rtmps://external-host:443/?rtmp://localhost:8506/
```

Remarque : *le fichier custom.ini respecte la casse ; utilisez des majuscules pour les noms de paramètre et des minuscules pour les valeurs.*

9 Enregistrez le fichier custom.ini.

10 Ouvrez le fichier VHost.xml situé dans le dossier *[rép_install_racine]*\comserv\win32\conf_defaultRoot__defaultVHost_ et enregistrez une copie de sauvegarde dans un autre emplacement.

11 Localisez la ligne suivante dans le fichier VHost.xml :

```
<RouteEntry></RouteEntry>
```

12 Remplacez la ligne de l'étape 11 par le code suivant :

```
<RouteEntry protocol="rtmp">*:*;*:${ORIGIN_PORT}</RouteEntry>
```

13 Enregistrez le fichier VHost.xml.

14 (Facultatif) Ouvrez le fichier VHost.xml dans un navigateur Web pour valider sa syntaxe.

15 Redémarrez Adobe Connect Pro Server 7 :

a Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server > Arrêter Connect Pro Central Application Server.

b Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server > Arrêter Connect Pro Meeting Server.

c Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server > Démarrer Connect Pro Meeting Server.

d Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server > Démarrer Connect Pro Central Application Server.

16 Ouvrez la Console de gestion des applications ((http://localhost:8510/console ou Démarrer > Programmes > Adobe Acrobat Connect Pro Server > Configurer Connect Pro Server 7).

17 Dans l'écran Paramètres de l'application, sélectionnez Paramètres du serveur et procédez comme suit :

a Entrez le nom de domaine pleinement qualifié de votre compte Connect Acrobat Pro dans la zone Hôte Connect Pro. Ce nom de domaine pleinement qualifié est l'URL avec laquelle les utilisateurs finaux se connectent à Acrobat Connect Pro.

b Entrez le nom de domaine pleinement qualifié du serveur de réunions Acrobat Connect Pro dans la zone Nom externe sous Mappages de l'hôte. Le serveur utilise cette valeur en interne.

Sécurisation du serveur d'applications uniquement

1 Ouvrez le fichier Adaptor.xml situé dans le dossier *[rép_install_racine]*\comserv\win32\conf_defaultRoot_ et enregistrez une copie de sauvegarde dans un autre emplacement.

2 Insérez le code suivant dans le fichier Adaptor.xml d'origine, à l'intérieur des balises `<Adaptor></Adaptor>` (remplacez le code en italique par vos propres valeurs) :

```
<SSL>
    <Edge name="applicationserver">
        <SSLServerCtx>

<SSLCertificateFile>[root_install_dir]\sslAppServerPublicCert.pem</SSLCertificateFile>
            <SSLCertificateKeyFile
type="PEM">[root_install_dir]\sslAppServerPrivateKey.pem</SSLCertificateKeyFile>
            <SSLPassPhrase>mypassphrase</SSLPassPhrase>
            <SSLCipherSuite>ALL:!ADH:!LOW:!EXP:!MD5:@STRENGTH</SSLCipherSuite>
            <SSLSessionTimeout>5</SSLSessionTimeout>
        </SSLServerCtx>
    </Edge>
</SSL>
```

Vous devez avoir deux fichiers : un pour le certificat SSL public et un pour la clé privée appartenant au certificat. Indiquez l'emplacement du certificat SSL public dans la balise `<SSLCertificateFile>`. Indiquez l'emplacement de la clé privée dans la balise `<SSLCertificateKeyFile>`. Le serveur envoie le certificat SSL public aux clients. La clé privée reste sur le serveur.

3 Localisez la ligne suivante dans le fichier Adaptor.xml :

```
<HostPort name="edge1">${DEFAULT_FCS_HOSTPORT}</HostPort>
```

4 Insérez le code suivant sous la ligne ajoutée à l'étape 3 :

```
<HostPort name="applicationserver" ctl_channel=":19351">:-443</HostPort>
```

5 Enregistrez le fichier Adaptor.xml.

6 (Facultatif) Ouvrez le fichier Adaptor.xml dans un navigateur Web pour valider sa syntaxe.

Si le navigateur signale une erreur, corrigez-la, puis rouvrez le fichier dans un navigateur Web. Répétez ce processus jusqu'à ce que le fichier soit valide.

7 Ouvrez le fichier custom.ini situé dans le répertoire d'installation racine (c:\breeze, par défaut) et enregistrez une copie de sauvegarde dans un autre emplacement.

8 Insérez le code suivant dans le fichier custom.ini, sans remplacer ni supprimer le texte existant :

```
ADMIN_PROTOCOL=https://
SSL_ONLY=yes
HTTPS_PORT=8443
```

Remarque : *le fichier custom.ini respecte la casse ; utilisez des majuscules pour les noms de paramètre et des minuscules pour les valeurs.*

9 Enregistrez le fichier custom.ini.

10 Redémarrez Acrobat Connect Pro Server 7.

a Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server > Arrêter Connect Pro Central Application Server.

b Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server > Arrêter Connect Pro Meeting Server.

c Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server > Démarrer Connect Pro Meeting Server.

d Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server > Démarrer Connect Pro Central Application Server.

Sécurisation du serveur de réunions uniquement

1 Ouvrez le fichier Adaptor.xml situé dans le dossier *[rép_install_racine]*\comserv\win32\conf_defaultRoot_ et enregistrez une copie de sauvegarde dans un autre emplacement.

2 Insérez le code suivant dans le fichier Adaptor.xml d'origine, à l'intérieur des balises `<Adaptor></Adaptor>` (remplacez le code en italique par vos propres valeurs) :

```
<SSL>
    <Edge name="meetingserver">
        <SSLServerCtx>

<SSLCertificateFile>[root_install_dir]\sslMeetingServerPublicCert.pem</SSLCertificateFile>
    <SSLCertificateKeyFile
type="PEM">[root_install_dir]\sslMeetingServerPrivateKey.pem</SSLCertificateKeyFile>
            <SSLPassPhrase>mypassphrase</SSLPassPhrase>
            <SSLCipherSuite>ALL:!ADH:!LOW:!EXP:!MD5:@STRENGTH</SSLCipherSuite>
            <SSLSessionTimeout>5</SSLSessionTimeout>
        </SSLServerCtx>
    </Edge>
</SSL>
```

Vous devez avoir deux fichiers : un pour le certificat SSL public et un pour la clé privée appartenant au certificat. Indiquez l'emplacement du certificat SSL public dans la balise `<SSLCertificateFile>`. Indiquez l'emplacement de la clé privée dans la balise `<SSLCertificateKeyFile>`. Le serveur envoie le certificat SSL public aux clients. La clé privée reste sur le serveur.

3 Localisez la ligne suivante dans le fichier Adaptor.xml :

```
<HostPort name="edge1">${DEFAULT_FCS_HOSTPORT}</HostPort>
```

4 Remplacez le code de l'étape 3 par :

```
<HostPort name="meetingserver" ctl_channel=":19350">:-443</HostPort>
```

5 Enregistrez le fichier Adaptor.xml.

6 (Facultatif) Ouvrez le fichier Adaptor.xml dans un navigateur Web pour valider sa syntaxe.

Si le navigateur signale une erreur, corrigez-la, puis rouvrez le fichier dans un navigateur Web. Répétez ce processus jusqu'à ce que le fichier soit valide.

7 Ouvrez le fichier VHost.xml situé dans le dossier *[rép_install_racine]*\comserv\win32\conf_defaultRoot__defaultVHost_ et enregistrez une copie de sauvegarde dans un autre emplacement.

8 Localisez la ligne suivante dans le fichier VHost.xml :

```
<RouteEntry></RouteEntry>
```

9 Remplacez la ligne de l'étape 8 par le code suivant :

```
<RouteEntry protocol="rtmp">*:*;*:${ORIGIN_PORT}</RouteEntry>
```

10 Enregistrez le fichier VHost.xml.

11 (Facultatif) Ouvrez le fichier VHost.xml dans un navigateur Web pour valider sa syntaxe.

12 Ouvrez le fichier custom.ini situé dans le répertoire d'installation racine (c:\breeze, par défaut) et enregistrez une copie de sauvegarde dans un autre emplacement.

13 Insérez le code suivant dans le fichier custom.ini, sans remplacer ni supprimer le texte existant :

```
RTMP_SEQUENCE=rtmps://external-host:443/?rtmp://localhost:8506/
```

14 Enregistrez le fichier custom.ini.

15 Redémarrez Acrobat Connect Pro Server 7.

a Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server > Arrêter Connect Pro Central Application Server.

b Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server > Arrêter Connect Pro Meeting Server.

c Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server > Démarrer Connect Pro Meeting Server.

d Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server > Démarrer Connect Pro Central Application Server.

Test de la configuration

1 Si vous avez sécurisé le serveur d'applications, connectez-vous à Connect Pro Central. Un cadenas apparaît dans votre navigateur.

2 Si vous sécurisez le serveur de réunions, accédez à une salle de réunion Acrobat Connect Pro. Un cadenas apparaît dans le témoin de connexion.

Configuration d'un protocole SSL matériel

Lorsque vous configurez un protocole SSL matériel, vous pouvez sécuriser le serveur d'applications (HTTP), le serveur de réunions (RTMP) ou les deux. Quelle que soit la configuration que vous choisissez, vous devez d'abord configurer le serveur DNS.

Pour plus d'informations sur la configuration de l'accélérateur matériel, consultez la documentation du fournisseur.

Configuration du serveur DNS

❖ Créez des entrées DNS pour tous les serveurs que vous planifiez de sécuriser.

Définissez un nom de domaine pleinement qualifié pour chaque serveur sécurisé (par exemple, application.exemple.com et réunion1.exemple.com).

Remarque : *dans un cluster de serveurs, tous les serveurs d'applications peuvent partager un certificat SSL, mais chaque serveur de réunions doit avoir son propre certificat SSL. Sur un même serveur, pour sécuriser à la fois les connexions HTTP (serveurs d'applications) et RTMP (serveur de réunions), vous devez avoir un total de deux noms de domaine pleinement qualifiés et deux certificats SSL (un pour chaque protocole).*

Configuration de SSL pour les serveurs de réunions et d'application

1 Configurez le périphérique matériel dans les objectifs suivants :

a Ecoutez le port 443 en externe pour application.exemple.com.

b Transmettez les données non chiffrées au serveur d'applications sur le port 8443.

c Ecoutez le port 443 en externe pour reunion1.exemple.com.

d Transmettez les données non chiffrées au serveur de réunions sur le port 1935.

e (Facultatif) Ecoutez le port 80 en externe pour application.exemple.com et transmettez les données non chiffrées au serveur d'applications sur le port 80. Le serveur d'applications redirige les utilisateurs vers le port 443.

2 Configurez le pare-feu dans les objectifs suivants :

a Autorisez le trafic vers le serveur d'applications sur le port 443 (et sur le port 80 si vous avez terminé l'étape 1e).

b Autorisez le trafic vers le serveur de réunions sur le port 443.

3 Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server > Configurer Connect Pro Server 7 pour ouvrir la Console de gestion des applications. Dans l'écran Paramètres de l'application, sélectionnez Paramètres du serveur et procédez comme suit :

a Entrez le nom de domaine pleinement qualifié du serveur d'applications (par exemple, connect.exemple.com) dans la zone Hôte Connect Pro. Ce nom de domaine pleinement qualifié est l'URL avec laquelle les utilisateurs finaux se connectent à Acrobat Connect Pro.

b Entrez le nom de domaine pleinement qualifié du serveur de réunions (par exemple, fms.exemple.com) dans la zone Nom externe sous Mappages de l'hôte. Le serveur utilise cette valeur en interne.

4 Ouvrez le fichier custom.ini situé dans le répertoire d'installation racine (c:\breeze, par défaut) et enregistrez une copie de sauvegarde dans un autre emplacement.

5 Insérez le code suivant dans le fichier custom.ini, sans remplacer ni supprimer le texte existant :

```
ADMIN_PROTOCOL=https://
SSL_ONLY=yes
HTTPS_PORT=8443
RTMP_SEQUENCE=rtmps://external-host:443/?rtmp://localhost:8506/
```

Remarque : *le fichier custom.ini respecte la casse ; utilisez des majuscules pour les noms de paramètre et des minuscules pour les valeurs.*

6 Enregistrez le fichier custom.ini.

7 Redémarrez Acrobat Connect Pro Server 7.

a Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server > Arrêter Connect Pro Central Application Server.

b Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server > Démarrer Connect Pro Central Application Server.

Configuration de SSL pour le serveur de réunions uniquement

1 Configurez le périphérique matériel dans les objectifs suivants :

a Ecoutez le port 443 en externe pour reunion1.exemple.com.

b Transmettez les données non chiffrées au serveur de réunions sur le port 1935.

2 Configurez le pare-feu pour autoriser le trafic vers le serveur de réunions sur le port 443.

3 Ouvrez le fichier custom.ini situé dans le répertoire d'installation racine (c:\breeze, par défaut) et enregistrez une copie de sauvegarde dans un autre emplacement.

4 Insérez le code suivant dans le fichier custom.ini, sans remplacer ni supprimer le texte existant :

```
RTMP_SEQUENCE=rtmps://external-host:443/?rtmp://localhost:8506/
```

5 Enregistrez le fichier custom.ini.

Configuration de SSL pour le serveur d'applications uniquement

1 Configurez le périphérique matériel dans les objectifs suivants :

a Ecoutez le port 443 en externe pour application.exemple.com.

b Transmettez les données non chiffrées au serveur d'applications sur le port 8443.

c (Facultatif) Ecoutez le port 80 en externe pour application.exemple.com et transmettez les données non chiffrées au serveur d'applications sur le port 80. Le serveur d'applications redirige les utilisateurs vers le port 443.

2 Configurez le pare-feu de manière à autoriser le trafic vers le serveur d'applications sur le port 443 (et sur le port 80 si vous avez terminé l'étape 1c).

3 Dans Acrobat Connect Pro, ajoutez le fichier custom.ini suivant dans le répertoire racine d'installation (C:\breeze, par défaut) :

```
ADMIN_PROTOCOL=https://
SSL_ONLY=yes
HTTPS_PORT=8443
```

Remarque : *le fichier custom.ini respecte la casse ; utilisez des majuscules pour les noms de paramètre et des minuscules pour les valeurs.*

4 Redémarrez Acrobat Connect Pro Server 7.

a Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server > Arrêter Connect Pro Central Application Server.

b Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server > Démarrer Connect Pro Central Application Server.

Test de la configuration

1 Si vous avez sécurisé le serveur d'applications, connectez-vous à Connect Pro Central. Un cadenas apparaît dans votre navigateur.

2 Si vous sécurisez le serveur de réunions, accédez à une salle de réunion Acrobat Connect Pro. Un cadenas apparaît dans le témoin de connexion.

Configuration du protocole SSL logiciel pour un serveur Edge

Si le protocole SSL logiciel est configuré sur le serveur d'origine, configurez l'authentification SSL logicielle pour chaque serveur Edge à sécuriser.

A l'instar d'un serveur d'origine, un serveur Edge comprend deux services : un service de réunion et un service d'application. Pour configurer SSL pour le service de réunion et le service d'application, il vous faut deux noms de domaine pleinement qualifiés et deux adresses IP. Vous pouvez partager le nom de domaine pleinement qualifié du service d'application avec le serveur d'origine, mais le service de réunion, en revanche, doit avoir son propre nom de domaine pleinement qualifié. Le nom de domaine pleinement qualifié du service d'application est l'URL avec laquelle les utilisateurs se connectent à leurs comptes Acrobat Connect Pro.

Par exemple, si vous avez un serveur Edge et un serveur d'origine, il vous faut trois noms de domaine pleinement qualifiés et trois certificats SSL : un pour chaque service de réunion et un pour les services d'application à partager. Il vous faut également quatre adresses IP : une pour chaque service de réunion et une pour chaque service d'application.

Dans cet exemple de configuration, le serveur d'origine a les adresses IP et les noms de domaine pleinement qualifiés suivants :

```
10.192.37.11 = connect.yourcompany.com
10.192.37.10 = meeting1.yourcompany.com
```

Le serveur Edge a les adresses IP et les noms de domaine pleinement qualifiés suivants :

```
10.192.37.100 = connect.yourcompany.com
10.192.37.101 = edge1.yourcompany.com
```

Remarque : *si vous installez le serveur Edge et le serveur d'origine pour la première fois, configurez les deux serveurs sans SSL et vérifiez qu'ils parviennent à communiquer ensemble. Une fois que la communication est établie, vous pouvez configurer SSL pour les deux serveurs.*

Voir aussi

« Déploiement de Connect Pro Edge Server » à la page 39

« A propos de la prise en charge SSL » à la page 81

Configuration du serveur Edge

1 Sur le serveur d'origine, ouvrez le fichier c:\[rép_install_racine]\comserv\win32\conf_defaultRoot_\Adaptor.xml. (Par défaut, *[rép_install_racine]* est *breeze*.) Copiez l'intégralité de la section `<SSL></SSL>`, comme suit :

```
<SSL>
    <Edge name="applicationserver">
        <SSLServerCtx>
        <SSLCertificateFile>C:\breeze\connect.yourcompany.com.pem</SSLCertificateFile>
            <SSLCertificateKeyFile type="PEM">C:\breeze\connect.yourcompany.comKEY.pem
            </SSLCertificateKeyFile>
            <SSLCipherSuite>ALL:!ADH:!LOW:!EXP:!MD5:@STRENGTH</SSLCipherSuite>
            <SSLSessionTimeout>5</SSLSessionTimeout>
        </SSLServerCtx>
    </Edge>
    <Edge name="meetingserver">
        <SSLServerCtx>
            <SSLCertificateFile>C:\breeze\meetingPublicCert.pem
            </SSLCertificateFile>
            <SSLCertificateKeyFile type="PEM">C:\breeze\meetingPrivateKey.pem
            </SSLCertificateKeyFile>
            <SSLPassPhrase></SSLPassPhrase>
            <SSLCipherSuite>ALL:!ADH:!LOW:!EXP:!MD5:@STRENGTH</SSLCipherSuite>
            <SSLSessionTimeout>5</SSLSessionTimeout>
        </SSLServerCtx>
    </Edge>
</SSL>
```

Remarque : *votre code peut contenir différentes valeurs, mais il doit contenir les mêmes éléments XML.*

2 Sur le serveur Edge, ouvrez le fichier c:\[rép_install_racine]\edgeserver\win32\conf_defaultRoot_\Adaptor.xml et collez le bloc de code `<SSL></SSL>` du serveur d'origine après la balise `<Adaptor>`.

3 Procédez comme suit pour configurer le service d'application et le service de réunion sur le serveur Edge :

a Le service d'application est la balise `<Edge name="applicationserver">` dans le bloc `<SSL>`. Le service d'application utilise le même nom de domaine pleinement qualifié que le service d'application sur le serveur d'origine. Copiez les fichiers .pem du certificat et de la clé du serveur d'origine vers le même emplacement sur le serveur Edge. Dans cet exemple, le nom de domaine pleinement qualifié est connect.votresociété.com.

```
<Edge name="applicationserver">
    <SSLServerCtx>
        <SSLCertificateFile>C:\breeze\connect.yourcompany.com.pem</SSLCertificateFile>
        <SSLCertificateKeyFile type="PEM">C:\breeze\connect.yourcompany.comKEY.pem
            </SSLCertificateKeyFile>
        <SSLCipherSuite>ALL:!ADH:!LOW:!EXP:!MD5:@STRENGTH</SSLCipherSuite>
        <SSLSessionTimeout>5</SSLSessionTimeout>
    </SSLServerCtx>
</Edge>
```

b Le service de réunion est la balise `<Edge name="meetingserver">` dans le bloc `<SSL>`. Modifiez le code XML pour que le service de réunion pointe vers des fichiers de certificat et de clé uniques pour son nom de domaine pleinement qualifié unique. Dans cet exemple, le nom de domaine pleinement qualifié est edge1.votresociété.com.

```
<Edge name="meetingserver">
    <SSLServerCtx>
        <SSLCertificateFile>C:\breeze\edge1.yourcompany.com.pem
        </SSLCertificateFile>
        <SSLCertificateKeyFile type="PEM">C:\breeze\edge1.yourcompany.comKEY.pem
        </SSLCertificateKeyFile>
        <SSLPassPhrase></SSLPassPhrase>
        <SSLCipherSuite>ALL:!ADH:!LOW:!EXP:!MD5:@STRENGTH</SSLCipherSuite>
        <SSLSessionTimeout>5</SSLSessionTimeout>
    </SSLServerCtx>
</Edge>
```

4 Dans le fichier Adaptor.xml sur le serveur Edge, localisez la ligne `<HostPort name="edge1">${FCS.HOST_PORT}</HostPort>`. Ajoutez les deux lignes ci-dessous à la suite :

```
<HostPort name="meetingserver" ctl_channel=":19354">206.192.37.100:-443</HostPort>
<HostPort name="applicationserver" ctl_channel=":19355">206.192.37.101:-443</HostPort>
```

Ce code relie les adresses IP internes du serveur Edge pour sécuriser le port 443. Cet exemple utilise les adresses IP internes 206.192.37.100 et 206.192.37.101. Dans votre code, remplacez les adresses IP internes de votre serveur Edge.

5 Enregistrez le fichier Adaptor.xml.

6 Ouvrez le fichier Adaptor.xml dans un navigateur Web pour vérifier que le code XML est valide.

S'il contient des erreurs de syntaxe, le navigateur Web affiche un message d'erreur. Corrigez les erreurs de code XML et revérifiez le fichier.

7 Sur le serveur Edge, ouvrez le fichier c:*[rép_install_racine]*\edgeserver\win32\conf_defaultRoot__defaultVHost_\Vhost.xml. Localisez la balise `<RouteEntry></RouteEntry>` et remplacez-la par ce qui suit :

```
<RouteEntry protocol="rtmp">*:*;10.192.37.11:8506</RouteEntry>
```

Ce code a pour effet que le serveur Edge dirige les connexions RTMP des adresses IP et des ports vers le serveur d'origine via le port 8506. Cet exemple utilise l'adresse IP 10.192.37.11. Dans votre code, remplacez l'adresse IP du service d'application sur le serveur d'origine.

8 Enregistrez le fichier VHost.xml.

9 Ouvrez le fichier Vhost.xml dans un navigateur Web pour vérifier que le code XML est valide.

S'il contient des erreurs de syntaxe, le navigateur Web affiche un message d'erreur. Corrigez les erreurs de code XML et revérifiez le fichier.

10 Sur le serveur Edge, ouvrez le fichier c:*[rép_install_racine]*\edgeserver\custom.ini.

11 Entrez le paramètre `FCS.HTTPCACHE_BREEZE_SERVER_SECURE_PORT` et définissez-le sur l'adresse IP ou le nom de domaine pleinement qualifié du serveur d'origine, comme dans l'exemple suivant :

```
FCS.HTTPCACHE_BREEZE_SERVER_SECURE_PORT=connect.yourcompany.com:443
FCS.HTTPCACHE_BREEZE_SERVER_NORMAL_PORT=connect.yourcompany.com:80
FCS_EDGE_HOST=edge1.yourcompany.com
FCS_EDGE_REGISTER_HOST=connect.yourcompany.com
FCS_EDGE_CLUSTER_ID=sanfran
FCS_EDGE_EXPIRY_TIME=60000
FCS_EDGE_REG_INTERVAL=30000
```

Si vous souhaitez configurer votre système pour se connecter via SSL uniquement, commentez le paramètre `FCS.HTTPCACHE_BREEZE_SERVER_NORMAL_PORT` comme suit :

```
# FCS.HTTPCACHE_BREEZE_SERVER_NORMAL_PORT=connect.yourcompany.com:80
```

***Remarque :** si le serveur Edge a des difficultés à résoudre le nom de domaine pleinement qualifié du serveur d'origine, utilisez l'adresse IP.*

12 Sur le serveur Edge, ouvrez le fichier C:\[rép_install_racine]\edgeserver\win32\conf\HttpCache.xml et mettez à jour la balise `<HostName>` comme suit :

```
<HostName>${FCS_EDGE_HOST}</HostName>
```

13 Enregistrez le fichier HttpCache.xml.

14 Ouvrez le fichier HttpCache.xml dans un navigateur Web pour vérifier que le code XML est valide.

S'il contient des erreurs de syntaxe, le navigateur Web affiche un message d'erreur. Corrigez les erreurs de code XML et revérifiez.

Configuration du serveur d'origine

1 Configurez le serveur d'origine pour SSL. Pour plus d'informations, reportez-vous à la section « Protocole SSL (Secure Sockets Layer) » à la page 81.

2 Sur le serveur d'origine, ouvrez le fichier c:\[rép_install_racine]\custom.ini et entrez ce qui suit pour lier le serveur Edge au serveur d'origine :

```
edge.FCS_EDGE_CLUSTER_ID=1
```

Utilisez la valeur du paramètre *`FCS_EDGE_CLUSTER_ID`* défini dans le fichier custom.ini sur le serveur Edge. Dans cet exemple, la valeur est `sanfran`, le code est donc `edge.sanfran=1`.

***Remarque :** la valeur 0 est réservée et ne peut pas être utilisée.*

3 Redémarrez Connect Pro Central Application Server et Connect Pro Meeting Server.

4 Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server > Configurer Connect Pro Server 7 pour ouvrir la Console de gestion des applications. Effectuez les opérations suivantes :

a Cliquez sur Paramètres du serveur.

b La zone Nom externe contient le nom de domaine pleinement qualifié du serveur Edge et une zone vide à droite. Si le nom de domaine pleinement qualifié n'apparaît pas, patientez quelques minutes et actualisez le navigateur.

c Entrez le nom de domaine pleinement qualifié du serveur Edge dans la zone vide, puis cliquez sur Enregistrer. Le serveur Edge est alors enregistré sur le serveur d'origine.

5 Configurez le serveur DNS local pour diriger les utilisateurs vers le serveur Edge lorsqu'ils demandent une URL Acrobat Connect Pro.

Configuration du protocole SSL matériel pour un serveur Edge

Si le protocole SSL matériel est configuré sur le serveur d'origine, configurez l'authentification SSL matérielle pour chaque serveur Edge à sécuriser.

A l'instar d'un serveur d'origine, un serveur Edge comprend deux services : un service de réunion et un service d'application. Pour configurer SSL pour le service de réunion et le service d'application, il vous faut deux noms de domaine pleinement qualifiés et deux adresses IP. Vous pouvez partager le nom de domaine pleinement qualifié du service d'application avec le serveur d'origine, mais le service de réunion, en revanche, doit avoir son propre nom de domaine pleinement qualifié. Le nom de domaine pleinement qualifié du service d'application est l'URL avec laquelle les utilisateurs se connectent à leurs comptes Acrobat Connect Pro.

Par exemple, si vous avez un serveur Edge et un serveur d'origine, il vous faut trois noms de domaine pleinement qualifiés et trois certificats SSL : un pour chaque service de réunion et un pour les services d'application à partager. Il vous faut également quatre adresses IP : une pour chaque service de réunion et une pour chaque service d'application.

Dans cet exemple de configuration, le serveur d'origine a les adresses IP et les noms de domaine pleinement qualifiés suivants :

```
10.192.37.11 = connect.yourcompany.com
10.192.37.10 = meeting1.yourcompany.com
```

Le serveur Edge a les adresses IP et les noms de domaine pleinement qualifiés suivants :

```
10.192.37.100 = connect.yourcompany.com
10.192.37.101 = edge1.yourcompany.com
```

***Remarque :** si vous installez le serveur Edge et le serveur d'origine pour la première fois, configurez les deux serveurs sans SSL et vérifiez qu'ils parviennent à communiquer ensemble. Une fois que la communication est établie, vous pouvez configurer SSL pour les deux serveurs.*

Voir aussi

« Déploiement de Connect Pro Edge Server » à la page 39

« A propos de la prise en charge SSL » à la page 81

Configuration du serveur Edge

1 Sur le serveur Edge, ouvrez le fichier c:\[rép_install_racine]\edgeserver\custom.ini.

2 Entrez le paramètre `FCS.HTTPCACHE_BREEZE_SERVER_SECURE_PORT` et définissez-le sur l'adresse IP ou le nom de domaine pleinement qualifié du serveur d'origine, comme dans l'exemple suivant :

```
FCS.HTTPCACHE_BREEZE_SERVER_SECURE_PORT=connect.yourcompany.com:443
FCS.HTTPCACHE_BREEZE_SERVER_NORMAL_PORT=connect.yourcompany.com:80
FCS_EDGE_HOST=edge1.yourcompany.com
FCS_EDGE_REGISTER_HOST=connect.yourcompany.com
FCS_EDGE_CLUSTER_ID=sanfran
FCS_EDGE_EXPIRY_TIME=60000
FCS_EDGE_REG_INTERVAL=30000
```

Si vous souhaitez configurer votre système pour se connecter via SSL uniquement, commentez le paramètre `FCS.HTTPCACHE_BREEZE_SERVER_NORMAL_PORT` comme suit :

```
# FCS.HTTPCACHE_BREEZE_SERVER_NORMAL_PORT=connect.yourcompany.com:80
```

***Remarque :** si le serveur Edge a des difficultés à résoudre le nom de domaine pleinement qualifié du serveur d'origine, utilisez l'adresse IP.*

3 Sur le serveur Edge, ouvrez le fichier C:\[rép_install_racine]\edgeserver\win32\conf\HttpCache.xml et mettez à jour la balise `<HostName>` comme suit :

```
<HostName>${FCS_EDGE_HOST}</HostName>
```

4 Enregistrez le fichier HttpCache.xml.

5 Ouvrez le fichier HttpCache.xml dans un navigateur Web pour vérifier que le code XML est valide.

S'il contient des erreurs de syntaxe, le navigateur Web affiche un message d'erreur. Corrigez les erreurs de code XML et revérifiez.

Configuration du serveur d'origine

1 Configurez le serveur d'origine pour SSL. Pour plus d'informations, reportez-vous à la section « Protocole SSL (Secure Sockets Layer) » à la page 81.

2 Sur le serveur d'origine, ouvrez le fichier c:\[rép_install_racine]\custom.ini et entrez ce qui suit pour lier le serveur Edge au serveur d'origine :

```
edge.FCS_EDGE_CLUSTER_ID=1
```

Utilisez la valeur du paramètre `FCS_EDGE_CLUSTER_ID` défini dans le fichier custom.ini sur le serveur Edge. Dans cet exemple, la valeur est `sanfran`, le code est donc `edge.sanfran=1`.

Remarque : *la valeur 0 est réservée et ne peut pas être utilisée.*

3 Redémarrez Connect Pro Central Application Server et Connect Pro Meeting Server.

4 Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server > Configurer Connect Pro Server 7 pour ouvrir la Console de gestion des applications. Effectuez les opérations suivantes :

a Cliquez sur Paramètres du serveur.

b La zone Nom externe contient le nom de domaine pleinement qualifié du serveur Edge et une zone vide à droite. Si le nom de domaine pleinement qualifié n'apparaît pas, patientez quelques minutes et actualisez le navigateur.

c Entrez le nom de domaine pleinement qualifié du serveur Edge dans la zone vide, puis cliquez sur Enregistrer. Le serveur Edge est alors enregistré sur le serveur d'origine.

5 Configurez le serveur DNS local pour diriger les utilisateurs vers le serveur Edge lorsqu'ils demandent une URL Acrobat Connect Pro.

Balises XML SSL

Balise	Valeur par défaut	Description
`SSLCertificateFile`	Aucune valeur par défaut.	Emplacement du fichier de certificat à envoyer au client. Lorsque aucun chemin absolu n'est spécifié, le certificat est supposé être situé dans le répertoire Adaptor.
`SSLCertificateKeyFile`	Aucune valeur par défaut.	Emplacement du fichier de la clé privée du certificat. Lorsque aucun chemin absolu n'est spécifié, le fichier de la clé est supposé être situé dans le répertoire Adaptor. Si le fichier de la clé est crypté, la phrase secrète doit être spécifiée dans la balise `SSLPassPhrase`. L'attribut `type` indique le type de codage utilisé pour le fichier de clé du certificat. Il peut s'agir de `PEM` ou de `ASN1`.
`SSLCipherSuite`	Voir la description.	Algorithme de chiffrement. L'algorithme est composé d'éléments séparés par des signes deux-points (:). Il peut s'agir d'algorithmes d'échange, de méthodes d'authentification, de méthodes de chiffrement, de types de résumés ou d'un nombre d'alias sélectionnés pour des regroupements courants. Pour obtenir la liste des composants, consultez la documentation de Flash Media Server. Cette balise présente le paramètre par défaut suivant : `ALL:!ADH:!LOW:!EXP:!MD5:@STRENGTH` Contactez l'assistance technique d'Adobe avant de modifier les paramètres par défaut.
`SSLPassPhrase`	Aucune valeur par défaut.	Phrase secrète à utiliser pour déchiffrer le fichier de la clé privée. Si le fichier de la clé privée n'est pas chiffré, laissez cette balise vide.
`SSLSessionTimeout`	5	Délai, en minutes, pendant lequel la session SSL demeure valide.

Paramètres de configuration SSL

Paramètre	Valeur par défaut	Description
`ADMIN_PROTOCOL`	`http://`	Protocole utilisé par le serveur d'application. Défini sur `https://` pour configurer SSL.
`DEFAULT_FCS_HOSTPORT`	`:1935`	Port utilisé par Flash Media Server pour communiquer via le protocole RTMP. Défini sur :-443,1935 pour configurer SSL.
`HTTPS_PORT`	Pas de valeur par défaut.	Port sur lequel le serveur d'application écoute les requêtes HTTPS. Ce paramètre est généralement défini sur `443` ou sur `8443` pour configurer SSL.
`SSL_ONLY`	`no`	Défini sur `yes` si le serveur ne prend en charge que les connexions sécurisées. Ce paramètre implique que toutes les URL Acrobat Connect Pro utilisent le protocole HTTPS.
`RTMP_SEQUENCE`	Pas de valeur par défaut.	Ports et points d'origine et d'extrémité utilisés pour se connecter au Flash Media Server (serveur de réunions).

Infrastructure à clé publique (ICP)

A propos de l'infrastructure à clé publique (ICP)

Vous pouvez configurer une infrastructure à clé publique (ICP) pour gérer les informations d'identification dans le cadre de l'architecture de sécurité Acrobat Connect Pro de vos clients. Dans le protocole SSL plus répandu, l'identité du serveur est vérifiée auprès du client ; dans une infrastructure à clé publique, l'identité du client est vérifiée auprès du serveur.

Une tierce partie approuvée, appelée autorité de certification, vérifie l'identité d'un client et lui associe un certificat. Le certificat (également appelé *clé publique*) est au format X.509. Lorsque le client se connecte à Acrobat Connect Pro, un proxy négocie sa connexion pour l'infrastructure à clé publique. Si le client dispose d'un cookie issu d'une session précédente ou d'un certificat valide, il est connecté à Acrobat Connect Pro.

Pour plus d'informations sur l'infrastructure à clé publique, consultez le Centre de technologie ICP de Microsoft.

Configuration requise ICP

Les utilisateurs doivent exécuter Windows XP ou Windows 2003 et avoir installé sur leur ordinateur local un certificat de client valide avant d'accéder à une réunion requérant une authentification ICP. Lorsque l'utilisateur accède à une réunion, une boîte de dialogue lui demande de choisir un certificat de client valide parmi ceux qui sont installés sur son ordinateur.

Adobe recommande que les clients utilisent Adobe Acrobat Connect Add-in pour participer aux réunions requérant des authentifications avec clé publique. Les clients doivent installer l'Add-in à l'aide de son programme d'installation autonome avant d'accéder à la réunion.

Les clients peuvent également utiliser la dernière version de Flash Player dans le navigateur pour accéder aux réunions, mais la prise en charge des clés publiques par Flash Player n'est pas aussi étendue que celle de l'Add-in. Cependant, pour afficher les archives de réunions, les clients doivent avoir installé la dernière version de Flash Player.

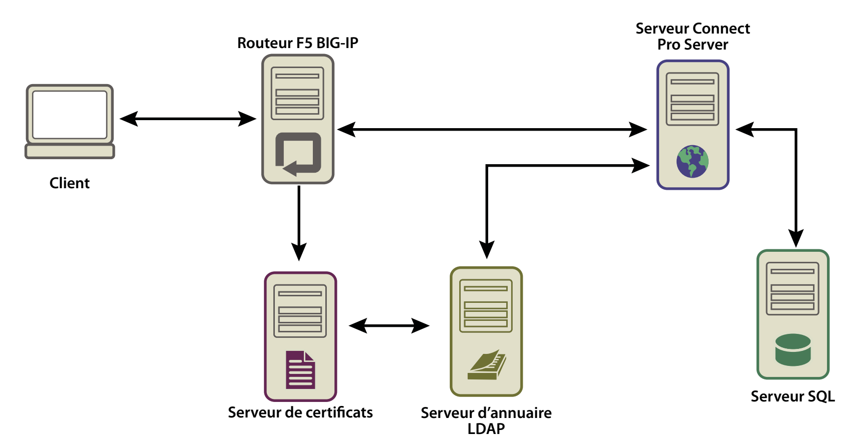
Vous pouvez concevoir un système ICP qui ne requiert que l'authentification des connexions HTTP ou des connexions HTTP et RTMP. Si vous exigez des certificats côté client pour les connexions HTTP et RTMP, le système interroge les utilisateurs à chaque nouvelle connexion au serveur. Par exemple, ils devront répondre à deux invites pour se connecter à une réunion, l'une pour HTTP et l'autre pour RTMP. La connexion RTMP ne pouvant pas être établie sans authentification HTTP, vous pouvez choisir d'exiger une authentification côté client uniquement pour la connexion HTTP.

Mise en œuvre de l'infrastructure à clé publique (ICP)

La procédure suivante vous guide tout au long de l'implémentation de l'infrastructure à clé publique (ICP) configurée avec un routeur F5 BIG-IP LTM 9.1.2 (version 40.2) comme proxy. Servez-vous des sections sensibles pour concevoir votre propre solution, avec un routeur F5 ou un autre périphérique.

Cette implémentation de référence respectent des normes de sécurité rigoureuses, par exemple, elle exige un certificat côté client pour les connexions HTTP (serveur d'applications) et RTMP (serveur de réunions).

Remarque : *Adobe vous recommande vivement d'adopter une stratégie de sécurité avant d'implémenter l'infrastructure à clé publique. Celle-ci exploite, en effet, un grand nombre de technologies différentes et le maintien de la sécurité est essentiel lors des interactions entre ces systèmes.*



Flux des données dans une infrastructure de clé publique

Cet exemple suppose la présence des éléments suivants :

- Acrobat Connect Pro est installé.
- Acrobat Connect Pro est intégré dans un service d'annuaire LDAP.
- Un utilisateur importé depuis le service d'annuaire LDAP peut accéder à une réunion d'Acrobat Connect Pro.
- Un routeur F5 est installé.

1. Configurez le serveur d'annuaire LDAP.

Un attribut LDAP `email` doit être spécifié pour chaque utilisateur. Cet attribut est ajouté dans le champ objet du certificat du client.

F5 iRule recherche l'adresse électronique dans X.509::objet et ajoute la valeur dans l'en-tête HTTP. Acrobat Connect Pro utilise l'en-tête HTTP pour authentifier l'utilisateur.

Remarque : *cet exemple utilise l'attribut* `email` *. Vous pouvez utiliser un identifiant unique quelconque au format X.509, d'une longueur maximale de 254 caractères et partagé par le service d'annuaire LDAP et Acrobat Connect Pro.*

2. Définissez la stratégie de connexion d'Acrobat Connect Pro.

Acrobat Connect Pro doit utiliser une adresse électronique comme identifiant de connexion de l'utilisateur. Dans Connect Pro Central, ouvrez l'onglet Administration, cliquez sur Utilisateurs et Groupes, puis sur Modifier les stratégies de nom d'utilisateur et de mot de passe.

3. Configurez un serveur d'autorité de certification.

Le serveur CA (Autorité de certification) traite les demandes de certificats, vérifie l'identité des clients, publie les certificats et gère la liste CRL (certificats révoqués).

Dans cette implémentation, le serveur CA s'adresse au serveur d'annuaire LDAP pour obtenir un certificat de client. Le serveur CA demande les informations du client au serveur LDAP et, si le client existe et n'a pas été révoqué, les met en forme dans un certificat.

Assurez-vous que le certificat du client soit installé et opérationnel en examinant le champ d'objet. Il doit se présenter comme suit :

```
E = adavis@asp.sflab.macromedia.com
CN = Andrew Davis
CN = Users
DC = asp
DC = sflab
DC = macromedia
DC = com
```

4. Configurez Acrobat Connect Pro pour qu'il utilise l'authentification des en-têtes HTTP.

Dans le fichier *[rép_install_racine]*\appserv\conf\WEB-INF\web.xml, retirez les commentaires du code suivant :

```
<filter-mapping>
    <filter-name>HeaderAuthenticationFilter</filter-name>
    <url-pattern>/*</url-pattern>
</filter-mapping>
```

Arrêtez le serveur de réunions et le serveur d'applications. Dans le fichier custom.ini du répertoire racine de l'installation, ajoutez la ligne suivante :

```
HTTP_AUTH_HEADER=hah_login
```

Enregistrez le fichier custom.ini et redémarrez Acrobat Connect Pro.

5. Configurez la logique applicative du routeur F5.

La logique applicative de F5 recherche l'adresse électronique dans le champ Objet du certificat du client. Elle transfère ensuite l'adresse électronique à Acrobat Connect Pro dans un en-tête HTTP supplémentaire.

Les clients qui ne possèdent pas de certificat sont rejetés. Lorsqu'un client possède un certificat, celui-ci doit être authentifié. OCSP (Online Certification Status Protocol) et la recherche LDAP sont des exemples de mécanismes d'authentification.

Une fois le certificat authentifié, recherchez-y un identifiant unique connu d'Acrobat Connect Pro. Dans cet exemple, une adresse électronique est recherchée dans un certificat valide.

Une requête qui inclut la chaîne `session` ou qui contient un cookie `BREEZESESSION` peut être transmise sans authentification car le client a déjà été authentifié. (Acrobat Connect Pro vérifie ces arguments par une requête à la base de données.)

Si la requête n'inclut pas la chaîne `session` ou le cookie `BREEZESESSION`, l'utilisateur doit se connecter à Acrobat Connect Pro. Pour connecter un utilisateur, placez l'identifiant unique (dans ce cas, l'adresse électronique) dans le champ `HTTP_AUTH_HEADER` et redirigez la requête vers la page de connexion de Connect Pro.

Le code suivant est un routeur F5 iRule placé dans le profil HTTPS qui gère les requêtes :

```
set id [SSL::sessionid]
set the_cert [session lookup ssl $id]
set uname [X509::subject $the_cert]
set emailAddr [getfield $uname "emailAddress=" 2]
if { [HTTP::cookie exists BREEZESESSION] } {
    set cookie_payload [HTTP::cookie value BREEZESESSION]
}
elseif { [HTTP::uri] contains "/system/login" }
{
    # Connection has been redirected to the "login page"
    # The email address has been parsed from the certificate
    #
    HTTP::header insert hah_login $emailAddr
}
elseif { [HTTP::uri] contains "session" }
{
    #do nothing, Acrobat Connect Pro verifies the token found in session=$token
}
else
{
    # URI encode the current request, and pass it to
    # the Acrobat Connect Pro system login page because the client
    # does not have a session yet.
    HTTP::redirect https://[HTTP::host]/system/login/ok?next=[URI::encode
https://[HTTP::host][HTTP::uri]]
}
```

Voir aussi

« Démarrage et arrêt de Connect Pro » à la page 103

Sécurisation de l'infrastructure

Sécurité du réseau

Pour ses communications, Acrobat Connect Pro s'appuie sur plusieurs services TCP/IP privés. Ces services ouvrent plusieurs ports et canaux qui doivent être protégés des utilisateurs extérieurs. Acrobat Connect Pro exige que vous placiez les ports sensibles derrière un pare-feu. Le pare-feu doit prendre en charge l'inspection de paquets avec état (pas seulement le filtrage des paquets). Une option du pare-feu doit permettre de « refuser tous les services par défaut à l'exception des services autorisés explicitement ». Le pare-feu doit être au moins un pare-feu à double interface (au moins deux interfaces réseau). Cette architecture permet d'éviter que des utilisateurs non autorisés ne contournent la sécurité du pare-feu.

La solution la plus simple pour sécuriser Acrobat Connect Pro consiste à bloquer tous les ports du serveur à l'exception des ports 80, 1935 et 443. Un pare-feu matériel externe offre un niveau de protection pour pallier les défectuosités du système d'exploitation. Vous pouvez configurer plusieurs couches de pare-feu matériel pour former des zones démilitarisées (DMZ). Si votre service informatique applique scrupuleusement tous les patchs de sécurité de Microsoft au serveur, il est possible de configurer un pare-feu logiciel pour assurer une sécurité supplémentaire.

Accès Intranet

Si certains de vos utilisateurs doivent accéder à Acrobat Connect Pro sur votre réseau Intranet, il est préférable de placer les serveurs Acrobat Connect Pro et leur base de données sur un sous-réseau distinct, isolé par un pare-feu. Le segment de réseau interne sur lequel est installé Acrobat Connect Pro doit utiliser des adresses IP privées (10.0.0.0/8, 172.16.0.0/12 ou 192.168.0.0/16) afin qu'il soit encore plus difficile pour un attaquant éventuel d'acheminer le trafic vers une adresse IP publique et depuis l'adresse IP réseau traduite en adresse IP interne. Pour plus d'informations, voir la rubrique RFC 1918. La configuration de ce pare-feu doit tenir compte de tous les ports d'Acrobat Connect Pro et de leur paramétrage pour un trafic entrant ou sortant.

Sécurité du serveur de base de données

Que vous hébergiez ou non votre base de données sur le même serveur qu'Acrobat Connect Pro, vous devez la protéger. Les ordinateurs hébergeant une base de données doivent être physiquement placés en un lieu protégé. Vous devez prendre les précautions supplémentaires suivantes :

- Installez la base de données dans la zone sécurisée de l'Intranet de votre société.
- Ne connectez jamais directement la base de données à Internet.
- Sauvegardez régulièrement toutes les données et stockez les copies dans un emplacement protégé hors site.
- Installez les derniers patchs publiés pour votre serveur de base de données.
- Utilisez des connexions SQL fiables.

Pour plus d'informations sur la sécurisation de SQL Server, rendez-vous sur le site Web consacré à la sécurité de Microsoft SQL.

Création de comptes de service

La création d'un compte de service pour Acrobat Connect Pro vous permet d'exécuter Acrobat Connect Pro de façon plus sécurisée. Adobe recommande la création d'un compte de service et d'un compte de service SQL Server 2005 Express Edition pour Acrobat Connect Pro. Pour plus d'informations, consultez les articles de Microsoft « Comment faire pour modifier le compte de service de SQL Server ou de l'Agent SQL Server sans utiliser SQL Enterprise Manager dans SQL Server 2000 ou le Gestionnaire de configuration SQL Server dans SQL Server 2005 » et « Le guide de la planification de la sécurité des services et des comptes de service ».

Création d'un compte de service

1 Créez un compte local appelé ConnectService et ne comprenant aucun groupe par défaut.

2 Définissez les services Adobe Connect Enterprise Server, Flash Media Administration Server et Flash Media Server (FMS) sur ce nouveau compte.

3 Définissez un « Contrôle total » pour la clé de registre suivante :

```
HKLM\SYSTEM\ControlSet001\Control\MediaProperties\PrivateProperties\Joystick\Winmm
```

4 Définissez un « Contrôle total » sur les dossiers NTFS du chemin du dossier racine d'Acrobat Connect Pro (C:\breeze, par défaut).

Les sous-dossiers et les fichiers doivent disposer des mêmes autorisations. Dans le cas de clusters, modifiez les chemins correspondants sur chaque nœud d'ordinateur.

5 Définissez les droits de connexion suivants pour le compte ConnectService :

Ouvrir une session en tant que service—SeServiceLogonRight

Création d'un compte de service SQL Server 2005 Express Edition

1 Créez un compte local appelé ConnectSqlService et ne comprenant aucun groupe par défaut.

2 Remplacez le compte de service SQL Server 2005 Express Edition Service Account de LocalSystem à ConnectSqlService.

3 Définissez un « Contrôle total » de ConnectSqlService pour les clés de registre suivantes :

```
HKEY_LOCAL_MACHINE\Software\Clients\Mail
HKEY_LOCAL_MACHINE\Software\Microsoft\Microsoft SQL Server\80
HKEY_LOCAL_MACHINE\Software\Microsoft\Microsoft SQL Server\[databaseInstanceName]
```

Pour les clusters, suivez cette procédure pour chaque nœud du cluster. L'autorisation Contrôle total s'applique à toutes les clés enfants d'une instance de base de données nommée.

4 Définissez un « Contrôle total » de ConnectSqlService pour les dossiers de la base de données. Les sous-dossiers et les fichiers doivent également disposer des mêmes autorisations. Dans le cas de clusters, modifiez les chemins correspondants sur chaque nœud d'ordinateur.

5 Définissez les droits d'utilisateur suivants pour le service ConnectSqlService :

Agir comme faisant partie du système d'exploitation—SeTcbPrivilege Outrepasser le contrôle de parcours—SeChangeNotify Verrouiller les pages en mémoire—SeLockMemory Ouvrir une session en tant que tâche—SeBatchLogonRight Ouvrir une session en tant que service—SeServiceLogonRight Remplacer un jeton au niveau du processus—SeAssignPrimaryTokenPrivilege

Sécurisation des installations à serveur unique

La procédure suivante résume le processus de configuration et de sécurisation d'Acrobat Connect Pro sur un ordinateur unique. Elle part du principe que la base de données est installée sur le même ordinateur et que les utilisateurs accèdent à Acrobat Connect Pro via Internet.

1. Installez un pare-feu.

Si vous autorisez les utilisateurs à se connecter à Acrobat Connect Pro via Internet, le serveur est à la merci des pirates informatiques. Un pare-feu vous permettra de bloquer l'accès au serveur et de contrôler les communications entre celui-ci et Internet.

2. Configurez le pare-feu.

Après avoir installé votre pare-feu, configurez-le comme suit :

- Ports d'entrée (depuis Internet) : 80, 443, 1935.
- Ports de sortie (vers le serveur de messagerie) : 25.
- Utilisez le protocole TCP/IP uniquement.

  La base de données étant située sur le même serveur qu'Acrobat Connect Pro, il n'est pas nécessaire d'ouvrir le port 1434 sur le pare-feu.

3. Installez Acrobat Connect Pro.

4. Vérifiez le bon fonctionnement des applications Acrobat Connect Pro.

Après avoir installé Acrobat Connect Pro, vérifiez qu'il fonctionne correctement depuis Internet et depuis votre réseau local.

5. Testez le pare-feu.

Une fois que vous avez installé et configuré le pare-feu, vérifiez qu'il fonctionne correctement. Testez le pare-feu en tentant d'utiliser les ports bloqués.

Sécurisation des clusters

Les systèmes de clusters (multi-serveurs) sont par nature plus complexes que les configurations à serveur unique. Un cluster Acrobat Connect Pro peut être situé dans un centre de données ou réparti géographiquement dans plusieurs centres d'exploitation du réseau. Vous pouvez installer et configurer les serveurs qui hébergent Connect Pro dans plusieurs sites et les synchroniser par l'intermédiaire d'une réplication de la base de données.

Remarque : *les clusters doivent utiliser Microsoft SQL Server 2005 Standard Edition, et non le moteur de base de données intégré.*

Conseils importants pour la sécurisation des clusters :

Réseaux privés La solution la plus simple pour les clusters situés sur le même site consiste à créer un sous-réseau supplémentaire pour le système Acrobat Connect Pro. Cette méthode offre un haut niveau de sécurité.

Pare-feux logiciels locaux Pour les serveurs Acrobat Connect Pro situés dans un cluster, mais partageant un réseau public avec d'autres serveurs, un pare-feu logiciel installé sur chaque serveur peut être approprié.

Systèmes VPN Dans les installations multi-serveurs hébergeant Acrobat Connect Pro dans des sites différents, vous pouvez envisager d'utiliser un canal chiffré pour communiquer avec les serveurs distants. De nombreux fournisseurs proposent des technologies VPN permettant de sécuriser les communications avec les serveurs distants. Si le trafic des données doit être chiffré, Acrobat Connect Pro s'appuie sur cette sécurité externe.

Ressources et conseils en matière de sécurité

Recommandations en matière de sécurité

La liste de contrôle suivante propose des recommandations pour la sécurisation de votre système Acrobat Connect Pro.

Protéger le trafic réseau par SSL Vous pouvez sécuriser la connexion avec le serveur de réunions, le serveur d'applications ou les deux.

Exécuter les services nécessaires uniquement N'exécutez pas d'applications, telles qu'un contrôleur de domaine, un serveur Web ou un serveur FTP, sur le même ordinateur qu'Acrobat Connect Pro. Pour minimiser les risques qu'une autre application soit utilisée pour compromettre le serveur, réduisez le nombre d'applications et de services exécutés sur l'ordinateur qui héberge Acrobat Connect Pro.

Mettre à jour la sécurité du système d'exploitation Vérifiez régulièrement la publication de mises à jour critiques corrigeant des failles de sécurité et appliquez les correctifs requis. Un pare-feu élimine certains de ces problèmes de sécurité. De façon générale, il est préférable d'appliquer à vos serveurs tous les correctifs de sécurité publiés et approuvés par Microsoft et les fournisseurs des autres plates-formes concernées.

Sécuriser les systèmes hôtes Si vous stockez des informations « sensibles » sur vos serveurs, veillez à la protection physique de vos systèmes. Acrobat Connect Pro dépend de la sécurisation de l'ordinateur hôte. Les serveurs doivent donc être protégés contre les intrusions s'ils contiennent des données personnelles et confidentielles. Acrobat Connect Pro est conçu pour tirer parti des fonctionnalités natives de l'environnement, telles que le chiffrement du système de fichiers.

Utiliser des mots de passe difficiles à déchiffrer Des mots de passe difficiles à déchiffrer protègent les données. Les administrateurs d'Acrobat Connect Pro peuvent définir des stratégies de mot de passe et de connexion dans Connect Pro Central. Les installations Acrobat Connect Pro utilisent souvent Microsoft SQL Server 2005 Standard Edition, qui requiert également une protection par des mots de passe difficiles à déchiffrer.

Utilisation d'une connexion LDAP ou d'une connexion unique pour l'authentification Il est recommandé d'utiliser une connexion LDAP ou une connexion unique pour l'authentification de Connect Pro. Si vous n'utilisez pas de connexion LDAP ni de connexion unique, assurez-vous que les utilisateurs finaux n'utilisent pas le même mot de passe pour Connect Pro que pour d'autres systèmes d'entreprise.

Effectuer des audits de la sécurité réguliers Il est recommandé d'effectuer régulièrement des audits des systèmes informatiques pour vérifier que toutes les mesures de sécurité prises fonctionnent comme prévu. Vous pouvez par exemple tester un pare-feu à l'aide d'un scanner de ports.

Références et ressources sur la sécurité

Les ressources suivantes peuvent vous aider à sécuriser vos serveurs.

Sécurisation du réseau L'Institut SANS (System Administration, Networking, and Security) est une organisation de coopération à vocation de recherche et de formation, constituée d'administrateurs système, de professionnels de la sécurité et d'administrateurs réseau. Cet institut propose des cours sur la sécurité des réseaux, ainsi qu'une certification en sécurité réseau.

Sécurisation de SQL Server La page relative aux ressources de sécurité Microsoft SQL du site Web de Microsoft fournit des informations sur la sécurisation de SQL Server.

Outils NMap est une puissante application de scanner qui signale tous les ports ouverts sur un ordinateur. Il est disponible gratuitement au titre de la licence publique GNU (GPL).

Remarque : *l'efficacité de toute mesure de sécurité dépend de nombreux facteurs, tels que les fonctions de sécurité assurées par le serveur et les logiciels de sécurité que vous avez installés. Le logiciel Acrobat Connect Pro n'est pas conçu pour assurer la sécurité de votre serveur et des informations qu'il renferme. Pour plus d'informations, consultez l'avis d'exonération de responsabilité de garantie, dans le contrat de licence applicable fourni avec Acrobat Connect Pro.*

Chapitre 5 : Administration de Connect Pro

L'administration de Connect Pro concerne les opérations suivantes :

- Gestion et surveillance de fichiers journaux pour gérer le temps de disponibilité du système
- Gestion de l'espace disque
- Sauvegarde de données
- Elaboration et génération de rapports sur l'utilisation

Démarrage et arrêt des serveurs

Démarrage et arrêt de Connect Pro

Vous pouvez démarrer ou arrêter Connect Pro via le menu Démarrer, la fenêtre Services ou la ligne de commande. Vérifiez que la base de données est en cours d'exécution avant de démarrer Connect Pro.

Arrêt de Connect Pro via le menu Démarrer

1. Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server > Arrêter Connect Pro Central Application Server.
2. Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server > Arrêter Connect Pro Meeting Server.

Démarrage de Connect Pro via le menu Démarrer

1. Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server > Démarrer Connect Pro Meeting Server.
2. Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server > Démarrer Connect Pro Central Application Server.

Arrêt de Connect Pro via la fenêtre Services

1. Choisissez Démarrer > Panneau de configuration > Outils d'administration > Services pour ouvrir la fenêtre Services.
2. Arrêtez le service Adobe Connect Enterprise Service.
3. Arrêtez le service Flash Media Server (FMS).
4. Arrêtez le service Flash Media Administration Server.

Démarrage de Connect Pro via la fenêtre Services

1. Choisissez Démarrer > Panneau de configuration > Outils d'administration > Services pour ouvrir la fenêtre Services.
2. Démarrez le service Flash Media Server (FMS).

3 Démarrez le service Flash Media Server Administration Server.

4 Démarrez le service Adobe Connect Enterprise Service.

Arrêt de Connect Pro via la ligne de commande

1 Choisissez Démarrer > Exécuter pour ouvrir la fenêtre Exécuter. Entrez **cmd** pour ouvrir une invite de commande.

2 Accédez au répertoire *[rép_install_racine]*\appserv\win32.

3 Entrez la commande suivante pour arrêter Connect Pro :

```
net stop ConnectPro
```

4 Pour arrêter Flash Media Server, tapez :

```
net stop FMS
```

5 Pour arrêter Flash Media Server Administration Server, tapez :

```
net stop FMSAdmin
```

Démarrage de Connect Pro via la ligne de commande

1 Choisissez Démarrer > Exécuter pour ouvrir la fenêtre Exécuter. Entrez **cmd** pour ouvrir une invite de commande.

2 Accédez au répertoire *[rép_install_racine]*\appserv\win32.

3 Pour démarrer Flash Media Server, tapez :

```
net start FMS
```

4 Pour démarrer Flash Media Server Administration Server, tapez :

```
net start FMSAdmin
```

5 Entrez la commande suivante pour démarrer Connect Pro :

```
net start ConnectPro
```

Démarrage et arrêt de Connect Pro Presence Service

Vous pouvez arrêter et démarrer Connect Pro Presence Service dans le menu Démarrer ou dans la fenêtre Services. Ne démarrez Connect Pro Presence Service que si votre système Connect Pro est intégré à Microsoft Live Communications Server ou à Office Communications Server.

Voir aussi

« Intégration à Microsoft Live Communications Server 2005 et Microsoft Office Communications Server 2007 » à la page 65

Arrêt du service de présence via le menu Démarrer

❖ Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server > Arrêter Connect Pro Presence Service.

Lancement du service de présence via le menu Démarrer

❖ Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server > Démarrer Connect Pro Presence Service.

Arrêt, démarrage ou redémarrage du service de présence via la fenêtre Services

1 Choisissez Démarrer > Panneau de configuration > Outils d'administration > Services pour ouvrir la fenêtre Services.

2 Sélectionnez Connect Pro Presence Service.

3 Sélectionnez Démarrer, Arrêter ou Redémarrer le service.

Démarrage et arrêt du service de téléphonie Connect Pro

Vous pouvez démarrer et arrêter le service de téléphonie Connect Pro via la fenêtre Services.

1 Choisissez Démarrer > Panneau de configuration > Outils d'administration > Services pour ouvrir la fenêtre Services.

2 Sélectionnez le service de téléphonie Acrobat Connect Pro.

3 Sélectionnez Démarrer, Arrêter ou Redémarrer le service.

Démarrage et arrêt de Flash Media Gateway

Vous pouvez démarrer et arrêter Flash Media Gateway depuis la fenêtre Services ou depuis la ligne de commande. Vérifiez que Connect Pro Server est exécuté avant de lancer Flash Media Gateway.

Démarrage et arrêt de Flash Media Gateway depuis la fenêtre Services

1 Choisissez Démarrer > Panneau de configuration > Outils d'administration > Services pour ouvrir la fenêtre Services.

2 Sélectionnez le service Flash Media Gateway.

3 Sélectionnez Démarrer, Arrêter ou Redémarrer le service

Démarrage et arrêt de Flash Media Gateway depuis la ligne de commande

1 Choisissez Démarrer > Exécuter pour ouvrir la fenêtre Exécuter. Entrez **cmd** pour ouvrir une invite de commande.

2 Pour démarrer Flash Media Gateway, tapez :

```
net start fmg
```

3 Pour arrêter Flash Media Gateway, tapez :

```
net stop fmg
```

Démarrage et arrêt de Connect Pro Server

Vous pouvez démarrer ou arrêter Connect Pro Edge Server 7 via le menu Démarrer, la fenêtre Services ou la ligne de commande.

Arrêt de Connect Pro Edge Server via le menu Démarrer

❖ Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Edge Server > Arrêter Connect Pro Edge Server.

Démarrage de Connect Pro Edge Server via le menu Démarrer

❖ Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Edge Server > Démarrer Connect Pro Edge Server.

Arrêt de Connect Pro Edge Server via la fenêtre Services

1 Choisissez Démarrer > Paramètres > Panneau de configuration > Outils d'administration > Services pour ouvrir la fenêtre Services.

2 Arrêtez le service Flash Media Server (FMS).

3 Arrêtez le service Flash Media Server Administration Server.

Démarrage de Connect Pro Edge Server via la fenêtre Services

1 Choisissez Démarrer > Paramètres > Panneau de configuration > Outils d'administration > Services pour ouvrir la fenêtre Services.

2 Démarrez le service Flash Media Server Administration Server.

3 Démarrez le service Flash Media Server (FMS).

Arrêt de Connect Pro Edge Server via la ligne de commande

1 Choisissez Démarrer > Exécuter pour ouvrir la fenêtre Exécuter. Entrez **cmd** pour ouvrir une invite de commande.

2 Pour arrêter Flash Media Server, tapez :

```
net stop FMS
```

3 Pour arrêter Flash Media Server Administrator Server, tapez :

```
net stop FMSAdmin
```

Démarrage de Connect Pro Edge Server via la ligne de commande

1 Choisissez Démarrer > Exécuter pour ouvrir la fenêtre Exécuter. Entrez **cmd** pour ouvrir une invite de commande.

2 Pour démarrer Flash Media Server Administrator Server, tapez :

```
net start FMSAdmin
```

3 Pour démarrer Flash Media Server, tapez :

```
net start FMS
```

Gestion et contrôle des fichiers journaux

A propos des fichiers journaux

Utilisez les fichiers journaux Connect Pro pour consulter les informations sur les événements qui se produisent pendant le fonctionnement. Vous pouvez utiliser ces informations pour créer des mécanismes de surveillance et des rapports, et pour résoudre des problèmes. Les fichiers journaux donnent des informations sur les activités des utilisateurs et sur les performances du serveur. Par exemple, les fichiers journaux peuvent indiquer pourquoi un utilisateur s'est vu refuser l'accès alors qu'il tentait de se connecter, ou les raisons de l'interruption des communications téléphoniques.

Connect Pro compte 5 fichiers journaux stockés dans le dossier *RootInstallationFolder*\logs. Pour surveiller Connect Pro, utilisez les fichiers access.log et error.log. Les trois autres fichiers journaux sont des fichiers internes qui n'ont pas d'impact sur le fonctionnement du système.

access.log Contient des informations sur les tentatives de connexion au serveur.

breeze.log Contient des informations sur le lancement, ou non, de l'application ConnectPro.exe.

error.log Contient des informations sur les problèmes liés au système.

service-err.log Contient les erreurs de démarrage et d'application.

service-out.log Contient les messages STDOUT et STDERR générés par la machine virtuelle Java (JVM).

Exemple d'entrée de fichier journal

L'exemple d'entrée ci-après, issu du fichier journal access.log, comprend un en-tête, une liste des champs utilisés dans l'entrée et des données spécifiques à cette entrée :

```
#Version: 1.0
#Start-Date: 2006-10-30 17:09:24 PDT
#Software: Adobe Acrobat Connect Pro Server
#Date: 2006-04-30
#Fields: date time x-comment x-module x-status x-severity x-category x-user x-access-request
time-taken db-logical-io db-transaction-update-count
2006-10-30 18:12:50 Not logged in. PRINCIPAL NO_ACCESS_NO_LOGIN W A PUBLIC
{cookie=breezxnb5pqusyshfgttt, ip=138.1.21.100} GET http://joeuser.macromedia.com&mode=xml 0
20/5 0
```

Le tableau suivant explique cet exemple.

Champ	Données	Description
date	2006-10-30	La date à laquelle l'événement consigné s'est produit.
time	18:12:50	L'heure à laquelle l'événement consigné s'est produit.
x-comment	Not logged in.	Indique qu'un utilisateur n'a pas pu se connecter au serveur d'application.
x-module	PRINCIPAL	L'événement s'est produit dans le module Principal du serveur d'application.
x-status	NO_ACCESS_NO_LOGIN	Indique que l'utilisateur n'a pas pu se connecter.
x-severity	W	Indique que l'événement est un avertissement (W pour « warning »).
x-category	A	Indique que l'événement représente un problème d'accès (A) (et qu'il apparaît donc dans le fichier journal access.log).
x-user	PUBLIC	L'utilisateur actuel ; dans ce cas, un invité non identifié ou un utilisateur public.
x-access-request	http://joeuser.macromedia.com&mode=xml	La source de la requête.
time-taken	0	La durée de traitement de cette requête est nulle.
db-logical-io	20/5	La requête a nécessité 20 consultations dans la base de données et 5 lignes de données ont été renvoyées.
db-transaction-update-count	0	Aucune ligne de données n'a été mise à jour pendant le traitement de la requête.

Rotation de fichiers journaux

Il est possible d'utiliser les fichiers journaux access.log et error.log en rotation. Modifiez les valeurs par défaut des paramètres suivants dans le fichier custom.ini (chemin d'accès par défaut : *RootInstallationFolder*\custom.ini) \custom.ini) afin de spécifier la fréquence de rotation des fichiers journaux :

```
ACCESS_LOG_ROTATE_DAYS=1.0
ACCESS_LOG_ROTATE_KEEP=7
ERROR_LOG_ROTATE_DAYS=1.0
ERROR_LOG_ROTATE_KEEP=7
```

Les paramètres `*_DAYS` déterminent la fréquence de rotation en jours des fichiers journaux. Pour une demi-journée, utilisez la valeur 0.5.

Les paramètres `*_KEEP` indiquent pendant combien de jours les fichiers journaux sont conservés avant leur suppression. Par défaut, les fichiers journaux sont conservés une semaine.

Une fois le fichier custom.ini modifié, redémarrez le serveur d'application de Connect Pro Central.

Format des fichiers journaux

Les fichiers journaux utilisent le format de fichier journal W3CExtended qui est lisible dans n'importe quel éditeur de texte.

Champs des fichiers journaux access.log et error.log

Chaque entrée de fichier journal contient 11 champs qui fournissent des informations sur le type de l'événement consigné, l'endroit où il s'est produit, son degré de sévérité et d'autres données pertinentes.

Champ	Format	Description
date	AAAA/MM/JJ	La date à laquelle la transaction s'est terminée.
time	HH:MM:SS	L'heure du système local à laquelle la transaction s'est terminée.
x-comment	Chaîne	Contient des informations intelligibles concernant l'entrée du fichier journal. Ce champ est toujours situé le plus à gauche possible.
x-module	Chaîne	Indique l'endroit où s'est produite l'erreur.
x-status	Chaîne	Indique le type d'événement qui est survenu.
x-severity	Texte (un caractère)	Indique si le degré de sévérité de l'événement consigné : C pour « Critical » (critique), E pour « Error » (erreur), W pour « Warning » (avertissement) ou I pour « Information ».
x-category	Texte (un caractère)	Indique si l'entrée du fichier journal représente un problème d'accès (A) ou système (S).
x-user	Chaîne	Indique l'utilisateur actuel. S'applique uniquement si la valeur de x-category est (A) ; autrement, la valeur de ce champ est un tiret (-), pour indiquer qu'il est inutilisé.
x-access-request	Chaîne	Indique la requête d'accès. Cette chaîne peut être une adresse URL ou le nom d'une API et un jeu de paramètres. S'applique uniquement si la valeur de x-category est (A) ; autrement, la valeur de ce champ est un tiret (-), pour indiquer qu'il est inutilisé.
time-taken	Chiffre	La durée de traitement de la requête (en secondes). S'applique uniquement si la valeur de x-category est (A) ; autrement, la valeur de ce champ est un tiret (-), pour indiquer qu'il est inutilisé.
db-logical-io	Chaîne	Le nombre de consultations de la base de données nécessaires au traitement de la requête et le nombre de lignes renvoyées, présentés sous la forme <reads>/<rows>.
db-transaction-update-count	Chaîne	Le nombre de lignes mises à jour dans les transactions pendant le traitement de la requête. Si la requête comprend plusieurs transactions, cette valeur est la somme de toutes les lignes mises à jour.

Entrées du champ Module

Un module est un composant du serveur qui gère un certain nombre d'opérations connexes. Chaque module appartient soit au serveur d'applications, soit au serveur de réunions. Le champ x-module indique l'endroit où s'est produit l'événement consigné.

Entrée de fichier journal pour le champ x-module	Description	Serveur
ACCESS_KEY	Gère les clés d'accès.	Serveur d'application
ACCOUNT	Gère les opérations liées aux comptes.	Serveur d'application
ACL	Gère les opérations liées à la liste de contrôle d'accès.	Serveur d'application
AICC	Gère toutes les communications AICC entre le serveur et les contenus.	Serveur d'application
BUILDER	Effectue les créations SCO.	Serveur d'application
Client	Méthodes client.	Serveur de réunions
CLUSTER	Gère toutes les opérations liées aux clusters.	Serveur d'application
CONSOLE	Gère toutes les opérations liées à la console.	Serveur d'application
Content	Module Partage.	Serveur de réunions
DB	Représente la base de données.	Serveur d'application
EVENT	Gère toutes les opérations liées aux événements.	Serveur d'application
HOSTED_MANAGER	Gère les comptes système (création, mise à jour, suppression, paramétrage, etc.).	Serveur d'application
MEETING	Gère toutes les opérations liées aux réunions.	Serveur d'application
Misc	Module d'opérations diverses.	Serveur de réunions
NOTIFICATION	Gère toutes les opérations liées aux e-mails.	Serveur d'application
PERMISSION	Gère toutes les opérations liées aux autorisations.	Serveur d'application
Poll	Module Sondage.	Serveur de réunions
PLATFORM_FRAMEWORK	Représente le cadre d'application de la plateforme.	Serveur d'application
PRINCIPAL	Gère toutes les opérations liées au module Principal.	Serveur d'application
REPORT	Représente les rapports.	Serveur d'application
Room	Gère le lancement et l'arrêt des salles de réunion.	Serveur de réunions
RTMP	Représente le gestionnaire RTMPHandler.	Serveur d'application
SCO	Gère toutes les opérations liées aux objets SCO.	Serveur d'application
SEARCH	Gère toutes les opérations de recherche.	Serveur d'application
START_UP	Représente le composant de démarrage.	Serveur d'application
TELEPHONY	Gère toutes les opérations de téléphonie.	Serveur d'application
TRACKING	Gère toutes les opérations liées aux transcriptions.	Serveur d'application
TRAINING	Gère toutes les opérations liées aux formations.	Serveur d'application

Entrées des champs Comment et Status

Les champs x-comment et x-status indiquent le type de l'événement consigné. Le champ x-status fournit un code pour chaque événement du fichier journal. Le champ x-comment fournit une description intelligible de l'événement.

Le tableau suivant répertorie les codes d'état, les commentaires associés à chaque code et une explication de chaque événement consigné.

Entrée de fichier journal pour le champ x-status	Entrée de fichier journal pour le champ x-comment	Description
ACCESS_DENIED	Client trying to access protected method. Access is denied. {1}	Consigné lorsqu'une machine client tente d'accéder à une méthode protégée.
BECAME_MASTER	Server {1} has been designated the master.	Consigné lorsque le planificateur se ferme et que le serveur considéré devient le planificateur.
CLUSTER_CON_BROKEN	Server {1} unable to reach {2} on port {3} to perform cluster operations.	Consigné lorsque Connect Pro est incapable de joindre un autre serveur du cluster.
CLUSTER_FILE_TRANSFER_ERROR	Unable to transfer {1} from server {2}.	Consigné lorsqu'une erreur est renvoyée lors du transfert d'un fichier.
CONNECT	New client connecting: {1}	Consigné lorsqu'une nouvelle machine client se connecte.
CONNECT_WHILE_GC	Connecting while the app is shutting down - forcing shutdown.	Consigné lorsqu'une machine client tente de se connecter pendant la fermeture de l'application.
DB_CONNECTION_ERROR	Unable to connect to database {1}.	Consigné lorsque Acrobat Connect ne parvient pas à établir une connexion à la base de données.
DB_CONNECTION_TIME_OUT	Timed out waiting for database connection.	Consigné lorsque l'établissement de la connexion à la base de données prend trop de temps.
DB_VERSION_ERROR	Database {1} is incompatible with the current version of Acrobat Connect Pro.	Consigné lorsque la base de données est obsolète.
DISCONNECT	A client is leaving. Details: {1}	Consigné lorsqu'une machine client se déconnecte.
EXT_ERROR	External error thrown by a third party.	Consigné lorsqu'un code externe renvoie une erreur.
FMS_CON_BROKEN	Health check failed due to broken FMS service connection.	Consigné lorsqu'une connexion de service est rompue.
FMS_NOT_FOUND	Unable to connect to FMS at startup.	Consigné lorsque Acrobat Connect ne peut établir de connexion de service au démarrage.
INTERNAL_ERROR	Internal error occurred.	Consigné lorsqu'une erreur interne est renvoyée.
INVALID	-	Consigné en cas de tentative d'opération non valide.
INVALID_DUPLICATE	Value {1} is a duplicate in the system.	Consigné lorsque la valeur entrée est identique à une valeur présente dans le système.

Entrée de fichier journal pour le champ x-status	**Entrée de fichier journal pour le champ x-comment**	**Description**
INVALID_FORMAT	Field {1} of type {2} is invalid.	La valeur spécifiée n'est pas valable pour ce champ.
INVALID_ILLEGAL_OPERATION	Illegal operation performed.	L'opération requise est illégale.
INVALID_ILLEGAL_PARENT	-	Consigné lorsqu'une liste de contrôle d'accès présente un parent non valide. Par exemple, si le dossier A se trouve à l'intérieur du dossier B, le dossier B ne peut se trouver dans le dossier A.
INVALID_MISSING	Field {1} of type {2} is missing.	Il manque une valeur obligatoire pour ce champ.
INVALID_NO_SUCH_ITEM	Value {1} is an unknown in the system.	L'élément requis n'existe pas.
INVALID_RANGE	The specified value must be between {1} and {2}.	Consigné lorsque la valeur entrée est hors plage.
INVALID_TELEPHONY_FIELD	Telephony authentication values were not validated by the service provider.	Le fournisseur de service n'est pas en mesure de valider le compte de téléphonie.
INVALID_VALUE_GTE	The specified value must be greater than or equal to {1}.	Consigné lorsque la valeur entrée est hors plage.
INVALID_VALUE_LTE	The specified value must be less than or equal to {1}.	Consigné lorsque la valeur entrée est hors plage.
KILLING_LONG_CONNECTION	Client has been in the room for 12 hours, disconnecting.	Consigné lorsque la connexion à la machine client a été interrompue suite à l'expiration du délai défini.
LICENSE_EXPIRED	Your license has expired and your account will be disabled on {1}. Please upload a new license file through the console manager to continue using Acrobat Connect Pro.	Consigné lorsque la licence Connect Pro d'une machine client arrive à expiration et que l'accès est sur le point d'être coupé.
LICENSE_EXPIRY_WARNING	Your license will expire on {1}. Please upload a new license file through the console manager to continue using Acrobat Connect Pro.	Consigné lorsque la période de validité de la licence est de 15 jours ou moins.
MASTER_THREAD_TIMED_OUT	Master thread has not reported progress in {1} milliseconds.	Le thread du planificateur ne s'exécute pas.
MEETING_BACKUP_END	Server {1} is no longer the backup for room {2}.	La sauvegarde de la réunion est arrivée à terme.
MEETING_BACKUP_START	Server {1} is now the backup for room {2}.	La sauvegarde de la réunion a débuté.
MEETING_FAILOVER	Meeting {1} failed over to {2}.	Consigné lorsqu'une réunion est reprise par ce serveur suite à un dysfonctionnement.
MEETING_TMP_READ	Meeting template {1} read for room {2}.	Lecture du modèle à partir de la réunion.
MEETING_TMP_WRITTEN	Meeting template {1} written to room {2}.	Ecriture du modèle pour la réunion.
NO_ACCESS_ACCOUNT_EXPIRED	Your account has expired.	Le compte d'accès a expiré.
NO_ACCESS_DENIED	Permission check failed.	Erreur de vérification des autorisations.
NO_ACCESS_LEARNER	No permission to take courses.	L'utilisateur doit faire partie du groupe des stagiaires pour participer à un cours.
NO_ACCESS_LEARNING_PATH_BLOCKED	You have not fulfilled a prerequisite or preassessment.	Erreur liée aux conditions ou évaluations préalables.

Entrée de fichier journal pour le champ x-status	**Entrée de fichier journal pour le champ x-comment**	**Description**
NO_ACCESS_NO_EXTERNAL_USER_MODIFICATION	External users cannot be modified.	L'utilisateur n'est pas autorisé à modifier les utilisateurs LDAP.
NO_ACCESS_NO_LICENSE_FILE	Your license file has not been uploaded.	Fichier de licence introuvable.
NO_ACCESS_NO_LOGIN	Not logged in.	Erreur renvoyée lorsque l'utilisateur n'est pas connecté.
NO_ACCESS_NO_QUOTA	A {1} quota error occurred for account {2} with limit {3}.	Quota dépassé.
NO_ACCESS_NO_RETRY	You have reached the max limit and can not take the course again.	L'utilisateur a dépassé le nombre maximal de cours.
NO_ACCESS_NO_SERVER	Server not available	Le serveur requis est indisponible.
NO_ACCESS_NOT_AVAILABLE	The requested resource is unavailable.	Consigné lorsque la ressource requise est indisponible.
NO_ACCESS_NOT_SECURE	SSL request made on a non-SSL server.	Une requête sécurisée a été effectuée sur un serveur non sécurisé.
NO_ACCESS_PASSWORD_EXPIRED	Your password has expired.	Consigné lorsque le mot de passe utilisateur a expiré.
NO_ACCESS_PENDING_ACTIVATION	Your account has not been activated yet.	Le compte n'est pas encore activé.
NO_ACCESS_PENDING_LICENSE	Your account activation is pending a license agreement.	Le compte est inutilisable tant que le contrat de licence n'a pas été lu.
NO_ACCESS_SCO_EXPIRED	The course you tried to access is no longer available.	La date de fin du cours est dépassée.
NO_ACCESS_SCO_NOT_STARTED	Course is not open yet.	La date de début du cours n'est pas encore atteinte.
NO_ACCESS_WRONG_ZONE	Content accessed from wrong zone.	Renvoyé lorsque l'accès au serveur s'effectue à partir d'une zone incorrecte.
NO_DATA	Permission check failed.	La requête n'a renvoyé aucune donnée.
NO_DISKSPACE	Health check failed due to lack of disk space.	Consigné lorsque l'espace disque réservé au compte est saturé.
NOT_AVAILABLE	Requested resource is not available.	Erreur renvoyée lorsque la ressource est indisponible.
OK	-	Requête traitée avec succès.
OPERATION_SIZE_ERROR	Operation too large to complete.	Consigné lorsque l'opération ne peut aboutir en raison de sa taille.
REQUEST_RETRY	Unable to process request. Please try again.	La requête a échoué.
RESPONSE_ABORTED	Client that made request is not available to receive response.	Consigné lorsque l'utilisateur ferme le navigateur avant que le serveur ait pu renvoyer une réponse.
RTMP_SVC_BLOCKED	Acrobat Connect Pro service request blocked from {1} because the server has not fully started up yet.	Une connexion de service a été requise à partir du module SCO mais le serveur est toujours en cours de démarrage.
RTMP_SVC_CLOSED	Acrobat Connect Pro service connection closed for {1}.	La connexion de service a été fermée pour le module SCO.

Entrée de fichier journal pour le champ x-status	Entrée de fichier journal pour le champ x-comment	Description
RTMP_SVC_REQUEST	Acrobat Connect Pro service request received from {1}.	Une connexion de service a été requise à partir du module SCO.
RTMP_SVC_START	Acrobat Connect Pro service connection established with {1}.	Une connexion de service a été établie avec le module SCO.
SCRIPT_ERROR	Run-Time Script Error. Details: {1}	Consigné lorsqu'une erreur de script est détectée.
SERVER_EXPIRED	Health check failed due to server expiry (expiry date={1}, current time={2}).	Consigné lorsque le contrôle de santé du serveur n'aboutit pas avant l'expiration du délai.
SOME_ERRORS_TERMINATED	Some actions terminated with an error.	Consigné lorsqu'une erreur entraîne l'arrêt de certaines opérations.
START_UP_ERROR	Start up error: {1}.	Consigné lorsqu'une exception est renvoyée lors du démarrage.
START_UP_ERROR_UNKNOWN	Unable to start up server. Acrobat Connect Pro might already be running.	Consigné lorsqu'une erreur est renvoyée lors du démarrage. JRUN imprime l'erreur.
TEL_CONNECTION_BROKEN	Telephony connection {1} was unexpectedly broken.	Consigné lorsque la connexion de téléphonie est rompue.
TEL_CONNECTION_RECOVERY	Telephony connection {1} was reattached to conference {2}.	Consigné lorsque Acrobat Connect rétablit une connexion à la conférence.
TEL_DOWNLOAD_FAILED	Unable to download {1} for archive {2}.	Consigné en cas d'expiration du délai pendant le téléchargement de fichier audio de téléphonie.
TOO_MUCH_DATA	Multiple rows unexpectedly returned.	Consigné lorsqu'une opération renvoie plus de données que prévu.
UNKNOWN_TYPE	{1}	Consigné lorsque le type de variable est inconnu.

Remarque : *dans le tableau ci-dessus, {1} et {2} représentent des variables remplacées par une valeur dans l'entrée du fichier journal.*

Entrées du champ Severity

Le champ x-severity indique le degré de sévérité d'une condition, ce qui vous aide à déterminer le niveau de réponse approprié.

Entrée de fichier journal pour x-severity	Significa-tion	Action suggérée	Exemple
C	Critique	Configurez des outils de surveillance tiers afin d'activer des systèmes d'alerte lorsque survient une entrée de fichier journal présentant ce degré de sévérité.	Impossible de joindre la base de données. Impossible de démarrer ou d'achever un processus. Le système connaît un dysfonctionnement.
E	Erreur	Configurez des outils de surveillance tiers afin d'envoyer un message électronique lorsque survient une entrée de fichier journal présentant ce degré de sévérité.	Impossible de joindre Adobe® Premiere®. Echec de la conversion. Un dysfonctionnement concerne un utilisateur ou un compte, mais pas l'intégralité du système.
W	Avertisse-ment	Générez et consultez des rapports périodiques afin d'identifier les améliorations du produit ou des fonctions à envisager.	L'utilisation du disque ou de la mémoire dépasse le seuil spécifié.
I	Infos	Consultez les entrées des fichiers journaux à des fins d'audit et de contrôle RCA.	Serveur démarré, arrêté ou redémarré.

Entrées du champ Category

Le champ x-category indique si l'événement correspond à un problème d'accès (A) ou un problème système d'ordre général (S). Toutes les entrées de catégorie A apparaissent dans le fichier journal access.log et toutes les entrées de catégorie S dans le fichier journal error.log.

Entrée de fichier journal pour le champ x-category	Signification	Description
A	accès	Le code d'état correspond à un problème d'accès. Consigné dans le fichier journal access.log.
S	système	Le code d'état correspond à un problème système. Consigné dans le fichier journal error.log.

Gestion de l'espace disque

A propos de la gestion de l'espace disque

Le système Connect Pro doit avoir un minimum d'1 Go d'espace disponible. Connect Pro n'intègre aucun outil de gestion de l'espace disque. Il appartient donc à l'administrateur d'utiliser des utilitaires du système d'exploitation ou des outils tiers pour surveiller l'espace disque disponible.

Le contenu peut être stocké sur le serveur qui héberge Connect Pro, sur des volumes de stockage externes, voire sur les deux.

Voir aussi

« Configuration du stockage partagé » à la page 59

Gestion de l'espace disque sur des serveurs Connect Pro

❖ Effectuez l'une des opérations suivantes :

- Utilisez Connect Pro Central pour supprimer du contenu inutilisé. Reportez-vous à Suppression d'un fichier ou d'un dossier.
- Remplacez votre disque serveur par un disque de plus grande capacité.

Remarque : *si l'espace disque disponible sur le serveur passe sous la barre de 1 Go, le serveur cesse de fonctionner.*

Gestion de l'espace disque sur des périphériques de stockage partagé

❖ Vérifiez si le périphérique de stockage partagé principal dispose de suffisamment d'espace libre et de nœuds de système de fichiers. Si l'une de ces deux valeurs passe sous la barre des 10 %, augmentez l'espace de stockage du périphérique ou ajoutez un autre périphérique de stockage partagé.

Remarque : *la valeur recommandée est de 10 %. Si vous utilisez un stockage partagé, veuillez également définir une valeur de taille de cache maximale dans la console de gestion des applications, sans quoi le cache risque d'occuper tout l'espace disque.*

Effacement du cache Edge Server

Adobe recommande de créer une tâche planifiée hebdomadaire pour effacer la mémoire cache des serveurs Edge. Il est judicieux d'exécuter cette tâche pendant les heures non travaillées, par exemple le dimanche matin.

1 Créez un fichier cache.bat afin de supprimer le répertoire de cache. L'entrée de ce fichier doit respecter la syntaxe suivante :

```
del /Q /S [cache directory]\*.*
```

Le répertoire cache par défaut se trouve à l'emplacement C:\breeze\edgeserver\win32\cache\http. Pour effacer le cache, utilisez la commande suivante :

```
del /Q /S c:\breeze\edgeserver\win32\cache\http\*.*
```

2 Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Edge Server > Arrêter Adobe Connect Pro Edge Server.

3 Exécutez le fichier cache.bat et vérifiez qu'il permet la suppression des fichiers présents dans le répertoire cache.

Remarque : *la structure du répertoire est conservée et tout fichier verrouillé par le Edge Server n'est pas effacé.*

4 Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Edge Server > Démarrer Adobe Connect Pro Edge Server.

5 Sélectionnez Démarrer > Panneau de configuration > Tâches planifiées > Ajouter une tâche planifiée.

6 Sélectionnez le fichier cache.bat en tant que nouveau fichier à exécuter.

7 Recommencez la procédure pour chaque Edge Server.

Sauvegarde de données

A propos de la sauvegarde de données

Il y a trois catégories de données que vous devez sauvegarder régulièrement : le contenu (tout fichier stocké dans les bibliothèques), les paramètres de configuration et les données de base de données.

Si vous n'utilisez pas de périphériques de stockage partagé, tout le contenu des bibliothèques est stocké dans le dossier *[rép_install_racine]*\content (C:\breeze\content, par défaut). Les paramètres de configuration sont stockés dans le fichier custom.ini situé dans le dossier d'installation racine (C:\breeze, par défaut).

L'exécution d'une copie de sauvegarde de la base de données crée une copie des données stockées dans la base de données. La planification de sauvegardes régulières de la base de données vous permet de récupérer à la suite de nombreuses pannes, dont des défaillances de support, des erreurs utilisateur et la perte définitive d'un serveur. Sauvegardez quotidiennement la base de données.

Vous pouvez également utiliser des sauvegardes pour copier une base de données d'un serveur sur un autre. Vous pouvez recréer la base de données complète à partir d'une sauvegarde en une seule étape, en restaurant la base de données. Le processus de restauration écrase la base de données existante ou crée la base de données si elle n'existe pas. La base de données rétablie correspond à l'état de la base de données au moment où la copie de sauvegarde a été effectuée, sans compter les transactions libres.

Vous créez des copies de sauvegarde sur des périphériques prévus à cet effet (disque ou bande). Vous pouvez utiliser un utilitaire SQL Server pour configurer vos sauvegardes. Par exemple, vous pouvez écraser des sauvegardes obsolètes ou annexer de nouvelles copies de sauvegarde au support.

Suivez les recommandations d'usage en ce qui concerne la sauvegarde de la base de données :

- Planifier une sauvegarde pendant la nuit.
- Conserver les sauvegardes dans un endroit sûr, de préférence dans un endroit différent du site où se trouvent les données.
- Conserver les anciennes sauvegardes pendant un certain temps au cas où la sauvegarde la plus récente serait endommagée, détruite ou perdue.
- Etablir un système pour écraser les sauvegardes en réutilisant les plus anciennes en premier. Utiliser des dates d'expiration sur les sauvegardes pour éviter l'écrasement prématuré.
- Etiqueter les supports de sauvegarde afin d'identifier les données et d'empêcher l'effacement de sauvegardes essentielles.

  Utilisez des utilitaires SQL Server pour sauvegarder la base de données :

- Transact-SQL
- SQL Distributed Management Objects (DMO)
- Assistant de création d'une sauvegarde de base de données
- SQL Server Management Studio

Sauvegarde de fichiers serveur

Sauvegardez et protégez les données système de la même manière que toutes les données de valeur de votre société.

Il est judicieux de planifier cette opération pendant la nuit.

1 Procédez comme suit pour arrêter Connect Pro :

a Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server > Arrêter le service Connect Pro Central.

b Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server > Arrêter le service de réunion Connect Pro.

2 Sauvegardez le répertoire de contenu.

L'emplacement par défaut est C:\breeze.

3 Sauvegardez le fichier custom.ini.

L'emplacement par défaut est C:\breeze\.

4 Procédez comme suit pour démarrer Connect Pro :

a Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server > Démarrer le service de réunion Connect Pro.

b Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server > Démarrer le service Connect Pro Central.

Sauvegarde de la base de données

Pour sauvegarder une édition de Microsoft SQL Server, vous pouvez utiliser Microsoft SQL Server Management Studio ou la fenêtre d'invite de commande.

L'édition de SQL Server qui s'installe avec Connect Pro Server ne comprend pas SQL Server Management Studio. Vous pouvez toutefois télécharger Microsoft SQL Server Management Studio Express de Microsoft.

Utilisation de SQL Server Management Studio pour sauvegarder SQL Server

Important : *ne désinstallez pas la base de données.*

1 Sous Windows, sélectionnez Démarrer > Programmes > Microsoft SQL Server 2005 > SQL Server Management Studio.

2 Dans l'arborescence de la fenêtre de l'explorateur d'objets, cliquez avec le bouton droit de la souris (nommé « breeze », par défaut) et choisissez Tâches > Sauvegarder...

Remarque : *pour des instructions complètes sur la sauvegarde et le rétablissement de la base de données SQL Server, consultez le site du support technique de Microsoft.*

Utilisation de la fenêtre d'invite de commande pour sauvegarder SQL Server

Pour accéder aux informations d'aide sur les commandes de base de données, tapez `osql ?` à l'invite DOS, puis appuyez sur Entrée.

Important : *ne désinstallez pas la base de données.*

1 Connectez-vous au serveur hébergeant Connect Pro Server.

2 Créez un dossier pour stocker les fichiers de sauvegarde de la base de données.

Cet exemple utilise le dossier C:\Connect_Database.

3 Sélectionnez Démarrer > Exécuter, tapez **cmd** dans la zone Ouvrir, puis cliquez sur OK.

4 A l'invite, indiquez le répertoire dans lequel vous avez installé la base de données. Le répertoire par défaut est c:\Program Files\Microsoft SQL Server\90\Tools\Binn.

5 A l'invite , entrez **osql -E** pour vous connecter au moteur de base de données et appuyez ensuite sur Entrée.

6 Entrez **BACKUP DATABASE nom de la base de données TO DISK = 'C:\Connect_Database\Nom_base de données.bak'** pour exécuter un utilitaire Microsoft SQL qui sauvegarde la base de données Connect, puis appuyez sur Entrée.

Le nom de la base de données par défaut est *breeze* .

7 A l'invite, tapez **go** et appuyez sur Entrée.

Le fenêtre de commande affiche des messages relatifs à la sauvegarde.

8 A l'invite, tapez **quit** et appuyez sur Entrée.

9 Pour vérifier que la sauvegarde a réussi, assurez-vous que le fichier breeze.bak est bien présent dans le répertoire C:\Connect_Database.

10 Pour redémarrer votre base de données, depuis le bureau de Windows, choisissez Démarrer > Panneau de configuration > Outils d'administration > Services. Dans la fenêtre Services, cliquez avec le bouton droit sur SQL Server (MSSQLSERVER) et choisissez Démarrer dans le menu contextuel.

Elaboration de rapports personnalisés

Elaboration de rapports personnalisés à l'aide de schémas en étoile

Connect Pro stocke les informations sur les utilisateurs, le contenu, les cours et les réunions dans une base de données. L'activité des utilisateurs fournit les données de la base. Vous pouvez utiliser des outils tels que Adobe® ColdFusion® Studio et Business Objects Crystal Reports pour interroger des schémas en étoile et afficher les données correspondantes. D'autres outils de type SQL sont également utilisables, tel SQL Query Analyser.

Les applications Connect Pro suivantes permettent de produire des rapports à partir des données disponibles :

Acrobat Connect Pro Meeting Participation, durée et contenu des réunions.

Adobe Presenter Affichage de contenus, de diapositives et de présentations.

Acrobat Connect Pro Training Informations destinées à la gestion des cours, telles que des statistiques sur les participants, sur l'affichage des contenus et les résultats des questionnaires.

Remarque : *vous pouvez en outre exécuter des rapports à partir de l'interface Web Connect Pro Central, puis les consulter en ligne ou les télécharger au format CSV. Pour plus d'informations, reportez-vous à la section* *Génération de rapports dans Connect Pro Central*.

Fait SCO

Colonne	Description
dim_sco_details_sco_id	Identifiant SCO
dim_sco_details_sco_version	Version SCO
max_retries	Nombre maximal de tentatives
owner_user_id	Identifiant utilisateur du propriétaire SCO
disk_usage_kb	Utilisation du disque en kilo-octets
passing_score	Note de césure
max_possible_score	Note maximale possible

Colonne	Description
views	Nombre de visualisations
unique_viewers	Nombre d'utilisateurs ayant visionné le SCO au moins une fois
slides	Nombre de diapositives
questions	Nombre de questions
max_score	Note maximale
min_score	Note minimale
average_score	Note moyenne
average_passing_score	Note de césure moyenne
total_registered	Note d'échec moyenne
total_participants	Nombre total d'utilisateurs inscrits
account_id	Nombre total de participants

Détails SCO

Colonne	Description
sco_id	Identifiant SCO
sco_version	Version SCO
sco_name	Nom
sco_description	Description
sco_type	Type SCO
sco_int_type	Type d'entier
is_content	Le SCO est-il un SCO de contenu ?
url	URL
parent_name	Nom du SCO parent
parent_sco_id	Identifiant du SCO parent
parent_type	Type du SCO parent
date_sco_created	Date de création
date_sco_modified	Date de modification
sco_start_date	Date de début
sco_end_date	Date de fin
version_start_date	Date de début de la version
version_end_date	Date de fin de la version
sco_tag_id	Identifiant de balise
passing_score	Note de césure
max_possible_score	Note maximale possible

Colonne	Description
linked_sco_id	Identifiant du SCO lié
linked_type	Type de SCO lié
owner_user_id	Identifiant de l'utilisateur propriétaire
storage_bytes_kb	Volume de stockage en kilo-octets
account_id	Identifiant de compte

Fait d'activité

Colonne	Description
dim_activity_details_activity_id	Identifiant d'activité
score	Note
passed	Réussi
completed	Achevé
peak_session_users	Pic d'utilisation de la session
number_correct	Nombre de réponses correctes
number_incorrect	Nombre de réponses incorrectes
number_of_questions	Nombre de questions
number_of_responses	Nombre de réponses
account_id	Identifiant de compte

Détails d'activité

Colonne	Description
activity_id	Identifiant d'activité
dim_sco_details_sco_id	Identifiant SCO
dim_sco_details_sco_version	Version SCO
dim_users_user_id	Identifiant utilisateur
dim_sco_details_parent_sco_id	Identifiant du SCO parent
score	Note
passed	Réussi
completed	Achevé
activity_type	Type d'activité
role	Rôle
date_activity_started	Date de début d'activité
date_activity_finished	Date de fin d'activité
dim_cost_center_id	Identifiant du centre de coûts
cost_center_audit_id	Identifiant d'audit

Colonne	Description
session_start_date	Date de début de la session
session_end_date	Date de fin de la session
attendance_activity	Est une activité de participation ?
session_id	Identifiant de session
account_id	Identifiant de compte

Examens de curriculums

Colonne	Description
dim_sco_details_curriculum_sco_id	Identifiant du curriculum
dim_sco_details_curriculum_sco_version	Version du curriculum
test_out_subject_sco_id	Identifiant du SCO objet
test_out_target_sco_id	Identifiant du SCO cible
test_out_type	Type d'examen
account_id	Identifiant de compte

Conditions préalables du curriculum

Colonne	Description
dim_sco_details_curriculum_sco_id	Identifiant du curriculum
dim_sco_details_curriculum_sco_version	Version du curriculum
pre_requisite_subject_sco_id	Identifiant du SCO objet
pre_requisite_target_sco_id	Identifiant du SCO cible
pre_requisite_type	Type de la condition préalable
account_id	Identifiant de compte

Conditions d'accomplissement requises pour le curriculum

Colonne	Description
dim_sco_details_curriculum_sco_id	Identifiant du curriculum
dim_sco_details_curriculum_sco_version	Version du curriculum
completion_subject_sco_id	Identifiant du SCO objet
completion_target_sco_id	Identifiant du SCO cible
completion_requirement_type	Type de conditions d'accomplissement requises
account_id	Identifiant de compte

Fait d'affichage en diapositives

Colonne	Description
dim_slide_view_details_slide_view_id	Identifiant de l'affichage en diapositives
dim_activity_details_activity_id	Identifiant d'activité
slide_view_display_sequence	Séquence d'affichage
account_id	Identifiant de compte

Détails d'affichage en diapositives

Colonne	Description
slide_view_id	Identifiant de l'affichage en diapositives
date_slide_viewed	Date d'affichage de la diapositive
slide_name	Nom de la diapositive
slide_description	Description de la diapositive
account_id	Identifiant de compte

Fait de réponses

Colonne	Description
dim_answer_details_answer_id	Identifiant de réponse
dim_activity_details_activity_id	Identifiant d'activité
dim_question_details_question_id	Identifiant de question
answer_display_sequence	Séquence d'affichage
answer_score	Note ?
answer_correct	Est correcte ?
account_id	Identifiant de compte

Détails de réponse

Colonne	Description
answer_id	Identifiant de réponse
date_answered	Date de la réponse
response	Réponse
account_id	Identifiant de compte

Fait de question

Colonne	Description
dim_sco_details_sco_id	Identifiant SCO
dim_sco_details_sco_version	Version SCO

Colonne	Description
dim_question_details_question_id	Identifiant de question
number_correct	Nombre de réponses correctes
number_incorrect	Nombre de réponses incorrectes
total_responses	Nombre total de réponses
high_score	Note élevée
low_score	Note faible
average_score	Note moyenne
account_id	Identifiant de compte

Détails des questions

Colonne	Description
question_id	Identifiant de question
question_display_sequence	Séquence d'affichage
question_description	Description
question_type	Type de question
account_id	Identifiant de compte

Réponses aux questions

Colonne	Description
dim_question_details_question_id	Identifiant de question
response_display_sequence	Séquence d'affichage des réponses
response_value	Valeur
response_description	Description
account_id	Identifiant de compte

Groupes

Colonne	Description
group_id	Identifiant du groupe
group_name	Nom du groupe
group_description	Description du groupe
group_type	Type de groupe
account_id	Identifiant de compte

Groupes d'utilisateurs

Colonne	Description
user_id	Identifiant utilisateur
group_id	Identifiant du groupe
group_name	Nom du groupe
account_id	Identifiant de compte

Utilisateur

Colonne	Description
user_id	Identifiant utilisateur
login	Nom de connexion
first_name	Prénom
last_name	Nom
email	Adresse de messagerie
user_description	Description de l'utilisateur
user_type	Type d'utilisateur
most_recent_session	Date de la session la plus récente
session_status	Etat de la session
manager_name	Nom du gestionnaire
disabled	Désactivé
account_id	Identifiant de compte
custom_field_1	Valeur du champ personnalisé 1
custom_field_2	Valeur du champ personnalisé 2
custom_field_3	Valeur du champ personnalisé 3
custom_field_4	Valeur du champ personnalisé 4
custom_field_5	Valeur du champ personnalisé 5
custom_field_6	Valeur du champ personnalisé 6
custom_field_7	Valeur du champ personnalisé 7
custom_field_8	Valeur du champ personnalisé 8
custom_field_9	Valeur du champ personnalisé 9
custom_field_10	Valeur du champ personnalisé 10

Noms de champs personnalisés

Colonne	Description
dim_column_name	Nom de colonne du champ personnalisé
custom_field_name	Nom du champ personnalisé

Colonne	Description
account_id	Identifiant de compte

Centres de coûts

Colonne	Description
cost_center_id	Identifiant du centre de coûts
cost_center_name	Nom du centre de coûts
cost_center_description	Description du centre de coûts

Création de rapports personnalisés à partir de vues de base de données héritées

Remarque : *Pour la première fois dans Connect Pro version 7, des schémas en étoile vous permettent d'élaborer des rapports personnalisés. Les vues de base de données existantes sont toujours prises en charge, mais les schémas en étoile constituent une solution normalisée plus robuste.*

Connect Pro stocke les informations sur les utilisateurs, le contenu, les cours et les réunions dans une base de données. L'activité des utilisateurs fournit les données de la base. Vous pouvez utiliser des outils tels que Adobe® ColdFusion® Studio et Business Objects Crystal Reports pour interroger la base de données et afficher les données correspondantes. D'autres outils de type SQL sont également utilisables, tel SQL Query Analyser.

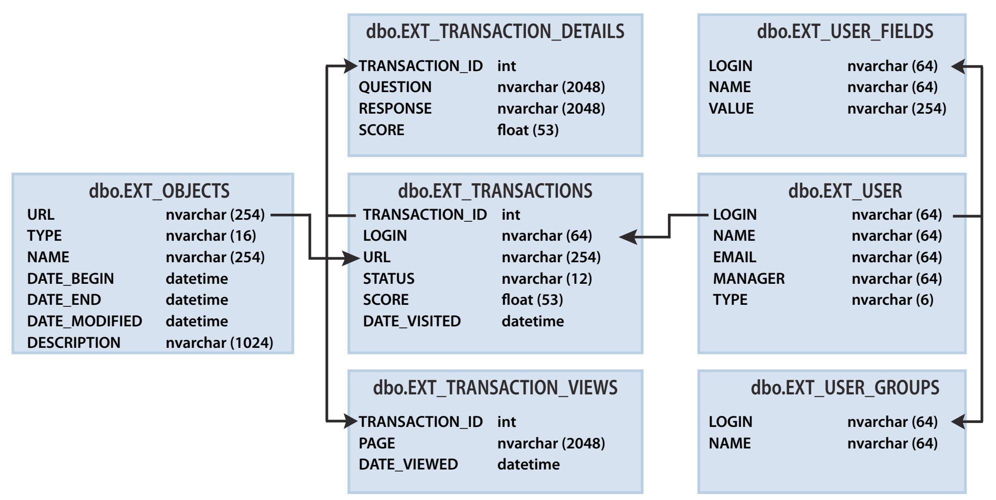
Les applications Connect Pro suivantes permettent de produire des rapports à partir des données disponibles :

Acrobat Connect Pro Meeting Participation, durée et contenu des réunions.

Adobe Presenter Affichage de contenus, de diapositives et de présentations.

Acrobat Connect Pro Training Informations destinées à la gestion des cours, telles que des statistiques sur les participants, sur l'affichage des contenus et les résultats des questionnaires.

Affichage des relations entre les vues de la base de données



Les flèches illustrent les relations d'entité existant entre les sept vues de rapport.

***Remarque :** éléments ou opérations non pris en charge : les vues non identifiées dans ce document, la modification des vues identifiées dans ce document ou l'accès direct au schéma de la base de données sous-jacente.*

❖ A l'aide d'un outil de schématisation se connectant à la base de données, vous pouvez afficher les relations existant entre les vues de la base de données.

EXT_TRANSACTIONS

Un identifiant de transaction unique est généré chaque fois qu'un utilisateur interagit avec un objet. La vue EXT_TRANSACTIONS renvoie les données répertoriées dans le tableau suivant.

Colonne	Type de données	Description
TRANSACTION_ID	INT	Identifiant unique de la transaction.
LOGIN	NVARCHAR	Nom de l'utilisateur ayant effectué cette transaction.
URL	NVARCHAR	Objet avec lequel l'utilisateur a interagi.
STATUS	NVARCHAR	Valeurs possibles : passed (réussi), failed (échoué), complete (terminé) ou in-progress (en cours).
SCORE	FLOAT	La note obtenue par l'utilisateur.
DATE_VISITED	DATETIME	Date de création ou de consultation de cette transaction.

Exemple de requête et données obtenues La requête suivante renvoie les données présentées dans le tableau ci-après.

```
select * from ext_transactions where url = '/p63725398/' order by login, date_visited asc;
```

TRANSACTION_ID	LOGIN	URL	STATUS	SCORE	DATE_VISITED
10687	test1-lnagaraj@test.enang.com	/p63725398/	in-progress	0.0	2006-12-15 00:56:16.500
10688	test1-lnagaraj@test.enang.com	/p63725398/	in-progress	0.0	2006-12-15 00:56:16.500
10693	test1-lnagaraj@test.enang.com	/p63725398/	in-progress	0.0	2006-12-15 00:58:23.920
10714	test1-lnagaraj@test.enang.com	/p63725398/	in-progress	10.0	2006-12-15 01:09:20.810
10698	test2-lnagaraj@test.enang.com	/p63725398/	in-progress	10.0	2006-12-15 01:00:49.483
10723	test3-lnagaraj@test.enang.com	/p63725398/	in-progress	10.0	2006-12-15 01:11:32.153
10729	test3-lnagaraj@test.enang.com	/p63725398/	completed	20.0	2006-12-15 01:12:09.700

Remarques relatives à la requête La vue EXT_TRANSACTIONS renvoie toutes les transactions existantes pour l'utilisateur et la session de formation donnés. Pour afficher la dernière transaction, vérifiez la valeur maximale de DATE_VISITED.

Vous pouvez filtrer les données en fonction des champs STATUS (Etat) et URL, afin d'obtenir une liste des utilisateurs ayant réussi la session de formation considérée, par exemple :

```
select * from ext_transactions where url = '/p31102136/' and status = 'user-passed' order by
login, date_visited asc;
```

Génération de données Actions de l'utilisateur permettant de générer des données dans cette vue :

- Participation à une réunion
- Affichage d'un élément de contenu
- Participation à une session de formation (cours ou curriculum)

Données exclues •Le numéro de certificat, qui n'existe pas dans la base de données

- La note maximale qui est le plus souvent indisponible

EXT_TRANSACTIONS_VIEWS

La vue EXT_TRANSACTIONS_VIEWS extrait les données concernant les diapositives ou les pages que les utilisateurs consultent.

Colonne	Type de données	Description
TRANSACTION_ID	INT	Identifiant unique de cette transaction (peut être fusionné avec TRANSACTION_DETAILS pour résumer par URL)
PAGE	NVARCHAR	Numéro de la diapositive ou de la page consultée.
DATE_VIEWED	DATETIME	Date de création de cette vue.

Exemple de requête et données obtenues La requête suivante renvoie les données présentées dans le tableau ci-après.

```
select * from ext_transaction_views where transaction_id = 10702 order by page asc;
```

TRANSACTION_ID	PAGE	DATE_VISITED
10702	0	2006-12-15 01:01:13.153
10702	1	2006-12-15 01:01:18.233
10702	2	2006-12-15 01:01:59.840
10702	3	2006-12-15 01:02:20.717

Génération de données Les données sont générées dans cette vue chaque fois qu'un utilisateur consulte du contenu ou une session de formation.

EXT_USERS

La vue EXT_USERS répertorie les utilisateurs et les attributs de profil associés :

Colonne	Type de données	Description
LOGIN	NVARCHAR	Identificateur d'utilisateur unique.
NAME	NVARCHAR	Nom d'utilisateur unique.
EMAIL	NVARCHAR	Adresse de messagerie unique.
MANAGER	NVARCHAR	ID d’ouverture de session du gestionnaire. Le gestionnaire est toujours défini sur NULL.
TYPE	NVARCHAR	Utilisateur ou invité. Le type est toujours défini sur utilisateur.

Exemple de requête et données obtenues La requête suivante renvoie les données présentées dans le tableau ci-après.

```
select * from ext_users;
```

LOGIN	NAME	EMAIL	MANAGER	TYPE
test4-lnagaraj@test.enang.com	test4 laxmi	test4-lnagaraj@test.enang.com	NULL	user
test7-lnagaraj@test.enang.com	TEST7 laxmi	test7-lnagaraj@test.enang.com	NULL	user

Génération de données Les données sont mises à jour dans la vue dès qu'un invité ou un utilisateur est créé, mis à jour ou supprimé.

Données exclues •Le mot de passe, qui n'est pas enregistré en texte standard.

- Le fuseau horaire et la langue, qui ne sont pas disponibles en version lisible ; par exemple, PST correspond à 323.
- La dernière connexion, trop lourde à calculer. Pour obtenir ce type de données, utilisez la requête `max(date_visited)` dans la vue EXT_TRANSACTION.
- La session active, c'est-à-dire les données issues de la vue EXT_TRANSACTIONS. Pour obtenir ce type de données, utilisez la requête `STATUS='IN-PROGRESS'` .
- Les utilisateurs supprimés n'apparaissent pas dans la vue EXT_USERS. Ils apparaissent en revanche dans la vue EXT_TRANSACTION.
- Les données relatives aux groupes ne sont pas incluses dans la vue.
- Les données relatives aux champs personnalisés créés ou prédéfinis. Pour chaque utilisateur, ces informations sont disponibles dans la vue EXT_USER_FIELDS.

EXT_USER_FIELDS

La vue EXT_USER_FIELDS répertorie pour chaque utilisateur les champs personnalisés créés ou prédéfinis. Elle comprend également les champs personnalisés des utilisateurs convertis en invités.

Colonne	Type de données	Description
LOGIN	NVARCHAR	Identificateur d'utilisateur unique.
NAME	NVARCHAR	Nom du champ, ex. numéro tél.
VALUE	NVARCHAR	Valeur du champ, ex. 07 66 77 99 57.

Exemple de requête et données obtenues La requête suivante renvoie les données présentées dans le tableau ci-après.

```
select * from ext_user_fields where login = 'test4-lnagaraj@test.enang.com';
```

LOGIN	NAME	VALUE
test4-lnagaraj@test.enang.com	{email}	test4-lnagaraj@test.enang.com
test4-lnagaraj@test.enang.com	{first-name}	test4
test4-lnagaraj@test.enang.com	{last-name}	laxmi
test4-lnagaraj@test.enang.com	{x-job-title}	sw engr 4
test4-lnagaraj@test.enang.com	{x-direct-phone}	NULL
test4-lnagaraj@test.enang.com	{x-direct-phone-key}	NULL
test4-lnagaraj@test.enang.com	SSN	777

Génération de données Actions permettant de générer des données dans cette vue : ajout, création ou mise à jour de champs personnalisés créés ou prédéfinis pour un ou plusieurs utilisateurs.

EXT_USER_GROUPS

La vue EXT_USER_GROUPS répertorie les données relatives aux groupes et aux membres associés. La vue EXT_USER_GROUPS utilise les données répertoriées dans le tableau suivant.

Colonne	Type de données	Description
LOGIN	NVARCHAR	Nom de l'utilisateur.
NAME	NVARCHAR	Nom du groupe.

Exemple de requête et données obtenues La requête suivante renvoie les données présentées dans le tableau ci-après.

```
select * from ext_user_groups where login = 'lnagaraj@adobe.com';
```

LOGIN	NAME
lnagaraj@adobe.com	{admins}
lnagaraj@adobe.com	{authors}
lnagaraj@adobe.com	{everyone}
lnagaraj@adobe.com	Laxmi Nagarajan

Remarques relatives à la requête L'imbrication de plusieurs groupes est prise en charge à partir de la version 5.1. Par exemple, si le groupe A contient le groupe B et que vous appartenez au groupe B, vous comptez aussi parmi les membres du groupe A.

Les groupes prédéfinis, tel le groupe Administrateurs, utilisent des noms de code dans le schéma, comme dans la requête SQL suivante : `SELECT * FROM EXT_USER_GROUPS where group='{admins}` . Le nom de code permet de distinguer les groupes prédéfinis des groupes créés par les utilisateurs.

Génération de données Actions de l'utilisateur permettant de générer des données dans cette vue :

- Création, mise à jour ou suppression d'un groupe
- Modification des membres d'un groupe

EXT_OBJECTS

La vue EXT_OBJECTS répertorie tous les objets du système (par exemple, les réunions, le contenu, les cours, etc.) et leurs attributs.

Colonne	Type de données	Description
URL	NVARCHAR	Identificateur unique de l'objet.
TYPE	NVARCHAR	Une présentation, un cours, un fichier FLV, un fichier SWF, une image, une archive, une réunion, un curriculum, un dossier ou un événement au choix.
NAME	NVARCHAR	Le nom de l'objet tel qu'affiché dans la liste de contenu.
DATE_BEGIN	DATETIME	La date de début prévue pour l'objet.
DATE_END	DATETIME	La date de fin prévue pour l'objet.
DATE_MODIFIED	DATETIME	La date de modification de l'objet.
DESCRIPTION	NVARCHAR	Les informations récapitulatives sur l'objet entré lors de la création d'une réunion, d'un contenu, d'un cours ou d'un autre type d'objet.

Exemple de requête et données obtenues La requête SQL suivante renvoie les données présentées dans le tableau ci-après :

```
select * from ext_objects order by type asc;
```

URL	TYPE	NAME	DATE_BEGIN	DATE_END	DATE_MODIFIED	DESCRIPTION
/p79616987/	cours	test api	2006-12-08 23:30:00.000	NULL	2006-12-08 23:36:55.483	NULL
/p47273753/	curriculum	test review curric	2006-12-14 21:00:00.000	NULL	2006-12-14 21:00:30.060	NULL
/tz1/	réunion	{default-template}	2006-12-12 19:15:00.000	2006-12-12 20:15:00.000	2006-12-12 19:25:07.750	présentation de version
/p59795005/	présentation	In-QUIZ-TEST1	NULL	NULL	2006-12-15 00:43:19.797	réunion de gestionnaires

Remarques relatives à la requête Vous pouvez obtenir tous les objets d'un type spécifique en filtrant les données selon le champ TYPE. Par exemple, la requête SQL suivante permet de filtrer les données pour afficher les cours et les curriculums.

```
select * from ext_objects where type in ('course', 'curriculum');
```

Pour obtenir la liste des types de systèmes disponibles, utilisez la requête SQL suivante :

```
select DISTINCT (type) from ext_objects;
```

Génération de données Actions de l'utilisateur permettant de générer des données dans cette vue :

- Création ou mise à jour d'une réunion, d'un cours ou d'un curriculum
- Transfert ou mise à jour de contenus

Données exclues •La durée, que vous pouvez calculer à l'aide de `date_end - date_begin` .

- La taille du disque, qui dévoilent les règles d'entreprise concernant l'opposition copies/originaux.
- L'identifiant du dossier.
- Les objets supprimés n'apparaissent pas dans la vue EXT_OBJECTS. Ils apparaissent en revanche dans la vue EXT_TRANSACTION.